به نام خدا

ایمن‌سازی مسیریابی SDN با استفاده از الگوریتم ژنتیک برای اینترنت اشیاء مبتنی بر بلاک‌چین

آرمین ترکمندی[1]، عرشیا رئوف پناه[2]

چکیده

اینترنت اشیاء (IoT) حوزه‌ای نوظهور است که در آن وسایل مختلف با حداقل دخالت انسان با یکدیگر ارتباط برقرار می‌کنند. دستگاه‌های اینترنت اشیاء معمولاً در محیط‌های خشن و بدون مراقبت کار می‌کنند. علاوه بر این، مسیریابی در معماری فعلی اینترنت اشیاء به دلیل وجود گره‌های مخرب و تأیید نشده، طول عمر کم شبکه، مسیریابی ناامن و غیره، ناکارآمد می‌شود. این مقاله یک مکانیزم احراز هویت سبک مبتنی بر بلاک‌چین را پیشنهاد می‌کند که در آن اعتبارنامه‌های حسگرهای معمولی ذخیره می‌شود. از آنجایی که عمر گره‌های اینترنت اشیاء به دلیل تمام شدن انرژی کوتاه است، اعتبارنامه‌های کمی برای دستیابی به احراز هویت سبک در بلاک‌چین ذخیره می‌شوند. علاوه بر این، محاسبه مسیر توسط یک کنترل‌کننده شبکه تعریف‌شده نرم‌افزاری (SDN) که از الگوریتم ژنتیک استفاده می‌کند، انجام می‌شود. این کنترل‌کننده همچنین برای مسیریابی بر حسب تقاضا برای بهینه‌سازی مصرف انرژی گره‌ها در شبکه اینترنت اشیاء استفاده می‌شود. همچنین، یک مکانیزم صحت مسیر برای بررسی وجود گره‌های مخرب در مسیر محاسبه‌شده پیشنهاد می‌شود. علاوه بر این، مکانیزم کشفی برای محدود کردن فعالیت‌های گره‌های مخرب پیشنهاد می‌شود، در حالی که لیستی از گره‌های مخرب در بلاک‌چین نگهداری می‌شود که در مکانیزم صحت مسیر استفاده می‌شود. مدل پیشنهادی با انجام شبیه‌سازی‌های فشرده ارزیابی می‌شود. اثربخشی مدل پیشنهادی از نظر مصرف گاز (Gas Consumption) نشان داده می‌شود که نشان‌دهنده استفاده بهینه از منابع است. انرژی باقی‌مانده شبکه، محاسبه بهینه مسیر را نشان می‌دهد، در حالی که روش تشخیص گره مخرب تعداد بسته‌های رها شده را نشان می‌دهد.

کلمات کلیدی

احراز هویت، بلاک چین، تکنیک های اکتشافی، اینترنت اشیاء، تشخیص گره های مخرب، صحت مسیر، شبکه تعریف شده توسط نرم افزار.

1- مقدمه

اکتشافات جغرافیایی در چند دهه‌ی اخیر محبوبیت زیادی پیدا کرده‌اند که با استفاده از دستگاه‌های اینترنت اشیا (IoT) مجهز به حسگرها انجام می‌شوند. همچنین پیش‌بینی شده که تا سال ۲۰۲۵، تعداد اتصالات IoT به ۳۰ میلیارد خواهد رسید [1]. علاوه بر این، IoT در حوزه‌های مختلفی مانند اینترنت اشیای صنعتی [2]، شهرهای هوشمند [3]، زنجیره غذایی کشاورزی [4] و غیره کاربردهای گسترده‌ای دارد. شبکه‌های IoT معمولاً در محیط‌های با دسترسی باز مانند شهرهای هوشمند، تولید غذا و تأمین انرژی عمل می‌کنند. بنابراین، شبکه IoT با مسائل زیادی روبرو است که توجه محققان را برای بهبود کارایی آن جلب می‌کند. چند دهه‌ی اخیر در تحقیقات IoT بسیار فعال بوده است که منجر به ارائه‌ی تعداد زیادی پروتکل‌های مسیریابی [5]، [6]، مدل‌های امنیتی [7]، [8] و تکنیک‌های خوشه‌بندی [9] شده که ارتباطات امن و قابل اعتماد را در شبکه‌های IoT فراهم می‌کنند. با این حال، شبکه‌های IoT همواره در معرض تهدید توسط گره‌های خارجی قرار دارند که با ارسال داده‌های نادرست به نفع خود، شبکه‌ها را گمراه می‌کنند. بنابراین، اگر تأیید هویت گره‌های رله (RNs) به درستی انجام شود، ترافیک می‌تواند به‌دقت مسیریابی شود. علاوه بر این، پروتکل‌های مسیریابی برای ارسال داده‌ها مورد نیاز هستند که توسط گره‌های رله مخرب تهدید می‌شوند.

در [10]، تأیید هویت گره‌ها با استفاده از یک مرجع متمرکز که نقطه‌ی شکست و اعتماد واحدی دارد، تضمین می‌شود. بنابراین، یک مکانیزم ذخیره‌سازی داده‌ی توزیع‌شده و مقاوم در برابر دستکاری مبتنی بر بلاکچین پیشنهاد شده است تا گره‌ها را تأیید هویت کند [11]. با این حال، شناسایی گره‌های مخرب داخلی به سادگی امکان‌پذیر نیست که باعث کاهش عملکرد کلی شبکه می‌شود [۱۲]. در ادبیات، مکانیزم‌های متمرکز زیادی برای شناسایی گره‌های مخرب داخلی پیشنهاد شده‌اند. با این حال، این مکانیزم‌ها به مسئله‌ی نقطه‌ی شکست واحدی که برای شبکه مضر است، دچار هستند [13]. در [14]، نویسندگان یک طرح تأیید هویت با استفاده از روش امضای گروهی پیشنهاد می‌کنند که به گره‌ها امکان عمل کردن به صورت مخرب را می‌دهد. دلیل آن این است که این گره‌ها می‌توانند پشت شناسه‌ی گروه پنهان شوند. علاوه بر این، نویسندگان در [15] یک طرح تأیید هویت مبتنی بر بلاکچین هیبریدی (HBA) پیشنهاد می‌دهند. با این حال، آنها رفتار مخرب گره‌های داخلی را که بر انتقال امن داده تأثیر می‌گذارد، در نظر نمی‌گیرند. علاوه بر این، در [16]، مسیر با استفاده از یک مدل یادگیری یافت می‌شود که طول عمر شبکه را کاهش می‌دهد. بلاکچین یک پلتفرم ذخیره‌سازی داده‌ی توزیع‌شده و امن است [17]، [18]، که هر گره یک نسخه از دفترکل غیرقابل تغییر که شامل تراکنش‌ها است، دارد [19]. بلوک‌ها با استفاده از آدرس‌های هش به هم متصل می‌شوند. هر بلوک هش بلوک قبلی خود را ذخیره می‌کند. هش یک بلوک با استفاده از اطلاعات ذخیره‌شده در آن تولید می‌شود و تغییر دادن داده‌های یک بلوک، هش آن را نیز تغییر می‌دهد. بنابراین، برای یک مهاجم امکان‌پذیر نیست که یک بلوک را بدون جلب توجه دستکاری کند [20]. از سوی دیگر، فناوری متمرکز دیگری به نام شبکه‌های تعریف‌شده توسط نرم‌افزار (SDN) برای مسیریابی داده استفاده می‌شود. در SDN، صفحه‌ی داده و صفحه‌ی کنترل از یکدیگر جدا هستند. روترهای صفحه‌ی داده دستگاه‌های بی‌هوشی هستند که فقط می‌توانند بسته‌ها را ارسال کنند، در حالی که در صفحه‌ی کنترل، یک کنترل‌کننده‌ی SDN مسئول تنظیم سیاست‌های مسیریابی است.

این مقاله بر تأیید هویت گره‌ها، بهینه‌سازی مسیریابی و شناسایی گره‌های مخرب یا مرده از مجموعه‌ای از گره‌ها تمرکز دارد. مکانیزم ثبت و تأیید هویت سبک مبتنی بر بلاکچین عمومی (LRA) برای محدود کردن گره‌های مخرب در مرحله‌ی اولیه پیشنهاد شده است. علاوه بر این، مکانیزم اجماع که توافق گره‌های شرکت‌کننده در درخواست تراکنش است، استفاده می‌شود. مکانیزم اجماع شناخته شده‌ی اثبات کار (PoW) در این کار پیشنهاد شده است تا بین موجودیت‌های توزیع‌شده اجماع ایجاد کند. این مکانیزم به توان محاسباتی بالا برای حل معمای از پیش تعریف شده نیاز دارد. این معما یک مسئله‌ی ریاضی است که حل آن دشوار و تأیید آن آسان است. نیاز به توان محاسباتی به سطح دشواری نانس از پیش تعریف شده بستگی دارد. گره‌های بلاکچین برای حل نانس و دریافت پاداش شرکت می‌کنند. نتیجه‌ی گره برنده توسط سایر گره‌های رقابتی در شبکه تأیید می‌شود. اگر ۵۱٪ از گره‌ها با نتیجه‌ی گره برنده موافقت کنند، گره برنده تراکنش را به بلوک اضافه کرده و پاداش دریافت می‌کند. به این ترتیب، یک بلاکچین ایجاد و نگهداری می‌شود. هک کردن بلاکچین مبتنی بر PoW برای مهاجمان چالش‌برانگیز است زیرا مهاجمان باید ۵۱٪ از گره‌های شبکه را به خطر بیاندازند که هم دشوار و هم پرهزینه است. علاوه بر این، الگوریتم ژنتیک (GA) [21] در کنترل‌کننده SDN، [23] برای یافتن مسیرهای بهینه برای ارسال داده استفاده می‌شود. کنترل‌کننده SDN با بلاکچین ادغام شده تا امنیت و صحت مسیرها را بررسی کند. برای ایمن‌سازی مسیر، کنترل‌کننده SDN مسیرها را به بلاکچین پخش می‌کند، جایی که صحت مسیر نیز با استفاده از مکانیزم صحت مسیر (RCM) بررسی می‌شود. اگرچه SDN یک فناوری متمرکز برای مسیریابی است [24]–[26]، سناریوی پیشنهادی شامل فناوری بلاکچین است تا شبکه را غیرمتمرکز کند.

جدول (1) : فهرست اختصارات و کلمات اختصاری

Abbreviation	Description
BS	Base Station
CH	Cluster Head
GA	Genetic Algorithm
HBA	Hybrid Blockchain based identity Authentication
IoT	Internet of Things
LRA	Lightweight Registration and Authentication
MND	Malicious Node Detection
PoA	Proof of Authority
PoS	Proof of Stake
PoW	Proof of Work
RNs	Relay Nodes
RCM	Route Correctness Mechanism
SDN	Software Defined Network
WSNs	Wireless Sensor Networks
$Crom(k,i)$	Next Hop in Route
C_i	Gene in the Selected Route k at ith hop
En_{RN}	Energy of RN
$Fitness(k)$	Fitness of kth route
ID_{RN}	ID of RN
k_{th}	The Number of Route
L_{RN}	Location of RN
MNL	Malicious Node's List

مشارکت‌های اصلی کار ما به شرح زیر است:

- مکانیزم LRA برای دستیابی به اعتماد در شبکه پیشنهاد شده است،
- مکانیزم مسیریابی مبتنی بر SDN و مجهز به GA برای یافتن مسیر بهینه استفاده شده است،
- مطالعات موردی مختلفی برای بررسی مقیاس‌پذیری مکانیزم مسیریابی پیشنهادی انجام شده است،

- RCM برای اعتبارسنجی مسیر محاسبه‌شده با استفاده از قرارداد هوشمند پیشنهاد شده است و
- گره‌های مخرب با استفاده از مکانیزم شناسایی گره‌های مخرب (MND) که بر اساس بسته‌های تأیید عمل می‌کند، شناسایی می‌شوند.

بقیه مقاله به شرح زیر سازماندهی شده است: بخش دوم به مرور ادبیات می‌پردازد. بخش سوم مدل سیستم پیشنهادی را مورد بحث قرار می‌دهد. بخش چهارم به ارزیابی عملکرد مدل سیستم پیشنهادی می‌پردازد. بخش پنجم جزئیات تحلیل امنیتی را ارائه می‌دهد و مقاله در بخش ششم نتیجه‌گیری می‌شود. فهرست اختصارات و مخففها در جدول (1) آمده است.

2- کارهای مرتبط

این بخش شامل مروری مختصر بر تلاش‌های تحقیقاتی مرتبط با اینترنت اشیا (IoT) و شبکه‌های حسگر بی‌سیم (WSNs) است. این تلاش‌ها بر اساس محدودیت‌های مورد بررسی دسته‌بندی شده‌اند.

2-1- مسیریابی مورد اعتماد برای اجتناب از گره‌های مخرب

2-1-1- مشکلات

در شبکه‌های حسگر بی‌سیم (WSNs)، موقعیت بیشتر گره‌های جدید ناشناخته است، بنابراین داده‌های تولید شده توسط آن‌ها تا زمانی که موقعیت مشخص نشود، بی‌فایده هستند. بسیاری از مکانیزم‌ها برای حل مشکل موقعیت‌یابی پیشنهاد شده‌اند، اما رفتار پویا گره‌ها، مکان‌یابی را چالش‌برانگیز می‌کند. علاوه بر این، مکان‌یابی بدون برد جذاب است زیرا کم‌هزینه و تطبیقی است. با این حال، ورود گره‌های مخرب عملکرد فرآیند مکان‌یابی را تحت تأثیر قرار می‌دهد [27]. همچنین، مکانیزم اعتبار برای گره‌های سیگنال‌دهنده جهت افزایش دقت مکان‌یابی ضروری است [28]. علاوه بر این، طبیعت پویا شبکه‌های WSN باعث افت بسته و کاهش صحت داده‌ها می‌شود. استفاده از سرگروه‌های متحرک باعث می‌شود که ارسال داده از نظر مصرف انرژی ناکارآمد باشد. همچنین، تعداد دستگاه‌های IoT روز به روز افزایش می‌یابد و این امر باعث می‌شود IoT بیشتر در معرض مسائل امنیتی مانند نقض حریم خصوصی قرار گیرد [29]. انواع مختلفی از حملات داخلی و خارجی ممکن است بر شبکه تأثیر بگذارد. همچنین، دو نوع روش تشخیص علیه حملات داخلی وجود دارد: روش‌های مبتنی بر پروتکل و روش‌های مبتنی بر اعتماد. با این حال، WSNها نیاز به روش‌های قابل اعتماد بیشتری برای شناسایی گره‌های مخرب دارند زیرا در یک محیط متمرکز، مسئله نقطه ضعف واحد وجود دارد [30]. طرح‌های مسیریابی موجود نمی‌توانند گره‌های مخرب را شناسایی کنند زیرا برخی از گره‌های مخرب می‌توانند خود را به عنوان گره‌های قانونی جا بزنند و در نتیجه اطلاعات مسیریابی نادرست را پخش کنند. بنابراین، مکانیزم‌های محاسبه ارزش اعتماد متمرکز توسط بسیاری از نویسندگان برای گره‌های همسایه پیشنهاد شده است. با این حال، این مکانیزم‌ها در ارتباط چندگامی سخت به کار می‌روند. همچنین، در صورت استفاده از یک شخص ثالث، دستیابی به سطوح قابل توجه از انصاف و شفافیت دشوار است [16]. شبکه‌های IoT با مسائلی مانند کمبود فضای ذخیره‌سازی، هزینه‌های بالای محاسباتی و تأخیر در محاسبات ابری مواجه هستند [31]. علاوه بر این، دو نوع رویکرد برای حفظ حریم خصوصی پیشنهاد شده است: متمرکز و غیرمتمرکز. سیستم متمرکز به دلیل وجود نقطه ضعف واحد، شکست می‌خورد، در حالی که سیستم غیرمتمرکز برای IoT مناسب نیست زیرا حجم زیادی از داده‌ها تولید می‌شود [32]. پروتکل‌های مسیریابی مبتنی بر بازخورد توسط طرح‌های موجود پیشنهاد شده‌اند که به دلیل بسته‌های بازخورد، بار کلی مسیریابی را افزایش می‌دهند. همچنین، ارسال مجدد به دلیل افت بسته منجر به مصرف انرژی بالای گره‌ها می‌شود [33]. مهاجمان می‌توانند به راحتی IoT و WSNها را به دلیل استقرار در محیط‌های سخت، مختل کنند که فرآیند مسیریابی را تحت تأثیر قرار می‌دهد. نویسندگان سیستم زیرساخت کلید عمومی با استفاده از مرجع مرکزی پیشنهاد می‌کنند. با این حال، فروشندگان مختلف به مرجع مرکزی به دلیل نقض داده اعتماد ندارند [34].

2-1-2- روش‌ها

مکانیزم ارزیابی اعتماد مبتنی بر بلاکچین در [27] پیشنهاد شده که از مسئله مشکل نقطه ضعف واحد جلوگیری می‌کند. علاوه بر این، مقادیر اعتماد گره‌ها از طریق انرژی باقیمانده، لیست همسایگان و تحرک محاسبه می‌شود. لیست همسایگان نیز برای محاسبه درجه گره به روز نگه داشته می‌شود. ارزش اعتماد ترکیبی بر اساس مدل تصمیم‌گیری مجموع وزن‌ها محاسبه می‌شود. برای اجماع، از اثبات سهام (PoS) استفاده می‌شود تا از هزینه محاسباتی بالای اثبات کار (PoW) جلوگیری شود. نویسندگان در [28] سه نوع مکانیزم ارزیابی اعتماد برای WSNها پیشنهاد می‌کنند: اعتماد مبتنی بر رفتار، اعتماد مبتنی بر بازخورد و اعتماد مبتنی بر داده. اعتماد مبتنی بر رفتار گره‌ها با استفاده از پارامترهای مختلفی از جمله نزدیکی به لحاظ فاصله، صداقت، زمان تعامل و فرکانس تعامل محاسبه می‌شود. در روش مبتنی بر بازخورد، اعتماد گره‌ها از طریق نرخ بازخورد مثبت و اعتبار محاسبه می‌شود. در نهایت، اعتماد مبتنی بر داده گره‌ها با استفاده از اعتماد مستقیم، اعتماد غیرمستقیم و زمان تعامل قبلی محاسبه می‌شود. یک مسیریابی سبک برای ارتباط امن بین گره‌ها به منظور افزایش عمر و کارایی شبکه ارائه شده است [29]. انتخاب سرگروه از طریق اصل عدم قطعیت انجام می‌شود. برخلاف راه‌حل‌های موجود، این مدل فناوری بلاکچین را با پروتکل مسیریابی ادغام می‌کند. علاوه بر این، سرگروه‌ها کلیدهای خصوصی برای امن‌سازی ارتباطات خود با ایستگاه پایه (BS) تولید می‌کنند. عملیات XOR برای محاسبه هش یکتا استفاده می‌شود که از نظر محاسباتی ناکارآمد است. بلاکچین عمدتاً برای ذخیره موقعیت‌ها، شناسه‌ها و غیره حسگرها استفاده می‌شود. نویسندگان در [30] یک مدل اعتماد مبتنی بر بلاکچین پیشنهاد می‌کنند که برخی از پارامترهای عملکردی تحویل بسته‌ها برای شناسایی گره‌های مخرب را محاسبه می‌کند. آستانه‌ای برای پارامترهای عملکرد بسته‌ها تعیین می‌شود. اگر مقادیر پارامترهای عملکرد بیش از آستانه باشد، سیستم گره را در شبکه لغو می‌کند. در [16]، نویسندگان مکانیزم غیرمتمرکزی پیشنهاد می‌کنند که سوابق مسیریابی چندگامی را نگه می‌دارد. در همین حال، نویسندگان از یادگیری تقویتی برای WSN بهره می‌برند. در هر مرحله از انتخاب گره بعدی، عامل یادگیری تقویتی یاد می‌گیرد و اطلاعات مسیریابی را در بلاکچین ذخیره می‌کند تا امنیت مسیر را تضمین کند. علاوه بر این، عامل برای هر اقدام موفق پاداش می‌گیرد. نویسندگان در [32] مکانیزم شناسایی گره‌های مخرب مبتنی بر بلاکچین و SDN غیرمتمرکز را

پیشنهاد می‌کنند. در مدل سیستم، از تکنیک‌های هوش مصنوعی برای ایجاد مدل‌های شناسایی استفاده می‌شود. مدل‌های شناسایی سپس در لایه مه با استفاده از بلاکچین به اشتراک گذاشته می‌شوند. علاوه بر این، کنترل‌کننده SDN سیاست‌های ارسال داده را از مدل شناسایی یاد می‌گیرد و به ترتیب به صفحه داده هدایت می‌کند. در همین حال، مدل‌های شناسایی همه شبکه‌های IoT بر روی لایه ابری ترکیب می‌شوند تا یک مدل واحد ایجاد شود. سپس، سیاست‌ها با هماهنگ‌سازی مدل‌های ابر با کنترل‌کننده‌های SDN در لایه مه ایجاد می‌شوند. کومار و همکاران [33] مکانیزم مسیریابی محلی مبتنی بر اعتماد با استفاده از طرح رمزنگاری پویا مبتنی بر بلاکچین را پیشنهاد می‌کنند. انتخاب مسیرها بر اساس ارزش اعتماد انجام می‌شود. مقادیر گره‌ها با استفاده از تعداد ارسال‌ها و ارسال‌های مجدد موفق اندازه‌گیری می‌شود. نویسندگان در [34] پروتکل مسیریابی قراردادی مبتنی بر بلاکچین توزیع‌شده برای شبکه IoT پیشنهاد می‌کنند. قراردادهای هوشمند برای کشف و ایجاد مسیر استفاده می‌شوند.

2-2- احراز هویت گره‌های شبکه

2-2-1- مشکلات

در مطالعات قبلی، مکانیزم‌های احراز هویت به دلیل استفاده از شخص ثالث مورد اعتماد، در معرض مشکل نقطه ضعف واحد قرار دارند. این مسئله با استفاده از بلاکچین با گره‌های ابری و مه حل می‌شود. با این حال، محیط بلاکچین به دلیل افزایش تعداد تراکنش‌های همزمان، نیازمند منابع زیادی است [15]. سیستم مدیریت کلید نیز به دلیل استقرار WSN در محیط‌های بحرانی و با دسترسی باز، به راحتی مورد حمله قرار می‌گیرد [35]. همچنین، دستگاه‌های IoT توسط فروشندگان مختلف تولید می‌شوند که قابلیت همکاری را مختل می‌کند زیرا گره‌ها به یکدیگر اعتماد ندارند. نویسندگان از طریق مکانیزم احراز هویت با مسائل قابلیت همکاری مقابله می‌کنند [36]. علاوه بر این، نیاز به ارتباط امن و بدون وقفه بین دستگاه‌ها در محیط IoT وجود دارد. دستگاه‌ها در معرض حملات مختلفی قرار دارند که می‌تواند باعث ایجاد فاجعه بزرگی شود. راه‌حل‌های متمرکز برای ایمن‌سازی ارتباطات پیشنهاد می‌شوند، اما این‌ها در معرض نقطه ضعف واحد قرار دارند [37].

2-2-2- روش‌ها

نویسندگان در [15] از یک بلاکچین ترکیبی استفاده می‌کنند که در آن گره‌ها بر اساس دامنه‌هایشان دسته‌بندی می‌شوند. ایستگاه‌های پایه به بلاکچین عمومی متصل هستند و برای ثبت و احراز هویت سرگروه‌ها استفاده می‌شوند. در مقابل، یک بلاکچین خصوصی بر روی سرگروه‌ها مستقر شده که ثبت و احراز هویت حسگرهای عادی را انجام می‌دهد. احراز هویت متقابل قبل از ارتباط بین دو گره انجام می‌شود. علاوه بر این، در [35]، زیرساخت کلید عمومی در OpenPGP برای دستیابی به محرمانگی استفاده می‌شود. از سوی دیگر، احراز هویت از طریق امضای دیجیتال انجام می‌شود. ارزیابی اعتماد مبتنی بر دانش استفاده می‌شود که در آن هر گره در مورد سایر گره‌ها بازخورد می‌دهد. بنابراین، جعل هویت یا ارائه داده‌های نادرست دشوار است. همچنین، نویسندگان در [36] پروتکل‌های احراز هویت همتا به همتا را پیشنهاد می‌کنند که در آن از بلاکچین برای احراز هویت گره‌ها در سطوح مختلف استفاده می‌شود. بلاکچین از الگوریتم درخت مرکل برای ذخیره اعتبار گره‌ها استفاده می‌کند و در صورت بروز اختلاف اقدام می‌کند. بلاکچین با IoT یکپارچه شده و از SHA-1 برای هش کردن اعتبار استفاده می‌شود. احراز هویت چند سطحی نیز در نظر گرفته شده تا گره‌ها بر اساس استقرارشان تقسیم شوند، در حالی که حمله‌های جمی برای بررسی اعتبار شبکه انجام می‌شود.

2-3- حفظ حریم خصوصی برای گره‌های بحرانی

2-3-1- مشکلات

در سنجش جمعی، دستگاه‌های موبایل برای جمع‌آوری داده‌ها استفاده می‌شوند. با این حال، آن‌ها داده‌های حساسی در مورد مالک خود دارند که ممکن است منجر به نشت اطلاعات خصوصی شود. بنابراین، چنین مسائلی کاربران را از شرکت در سنجش جمعی بی‌انگیزه می‌کند [38], [39]. علاوه بر این، کلیدهای رمزنگاری برای دستیابی به ارتباط امن بین لایه‌های مختلف گره‌ها در WSNها استفاده می‌شوند. با این حال، کلیدهای متقارن نیاز به ذخیره‌سازی اضافی و یک کانال امن برای به اشتراک‌گذاری داده‌ها دارند. در مقابل، رمزنگاری نامتقارن مشکلات مدیریت کلید را به همراه دارد زیرا گره‌های عادی می‌توانند در حین فرآیند تولید کلید، کلیدها را جعل کنند. علاوه بر این، طرح‌های حفظ حریم خصوصی توزیع‌شده منجر به بار اضافی ذخیره‌سازی می‌شوند [40]. همچنین، شهرهای هوشمند به پهنای باند بالا نیاز دارند که برای جمعیت رو به افزایش ضروری است. علاوه بر این، تأخیر کم، تحرک بالا، مقیاس‌پذیری ساختاری و نقطه ضعف واحد به دلیل معماری متمرکز نیز از مشکلات رایج در شهرهای هوشمند هستند. در همین حال، حفظ حریم خصوصی و امنیت گره‌ها به دلیل جمع‌آوری حجم بالای داده‌ها ممکن است به خطر بیفتد [41].

2-3-2- روش‌ها

یک مکانیزم انگیزشی مبتنی بر بلاکچین برای حفاظت از اطلاعات خصوصی گره‌ها پیشنهاد شده است [38]. مکانیزم سردرگمی به سیستم اضافه شده تا اطلاعات گروه را محافظت کند. SHA-256 دوبل برای هش کردن اطلاعات کاربران استفاده می‌شود که به صورت شفاف در بلاکچین ذخیره می‌شود. هر اطلاعات هش شده در درخت مرکل ذخیره می‌شود که در صورت بروز اختلاف قابل ردیابی است. علاوه بر این، زمانی که گره‌ها وظایف را ارسال می‌کنند، ارز مجازی قابل تبدیل به حساب‌های گره‌ها توسط بلاکچین منتقل می‌شود. نویسندگان در [40] یک طرح مدیریت کلید امن مبتنی بر بلاکچین را پیشنهاد می‌کنند. سطوح مختلف حسگرها برای کاهش بار محاسباتی ایستگاه‌های پایه استفاده می‌شوند. علاوه بر این، رمزنگاری متقارن به جای رمزنگاری نامتقارن استفاده می‌شود به دلیل کمبود منابع. در IoT و شهرهای هوشمند [41]، حجم زیادی از داده‌ها تولید و در یک نقطه متمرکز جمع‌آوری می‌شود. بنابراین، داده خام به لایه لبه برای پیش‌پردازش بارگذاری می‌شود. در لایه لبه، داده‌ها توسط ماینرهای لبه تجمیع و تأیید می‌شوند از طریق Itsuku PoW. در همین حال، SDN و بلاکچین به صورت همزمان کار می‌کنند تا یک محیط توزیع‌شده و امن در شهرهای هوشمند ایجاد کنند. SDN عمدتاً برای دستیابی به مقیاس‌پذیری معماری شبکه با مسیریابی داده‌ها از یک نقطه استفاده می‌شود.

2-4- مکانیزم‌های سبک برای بهبود سازگاری

2-4-1- مشکلات

بلاکچین نیاز به دستگاه‌های مجهز به منظور انجام وظایف محاسباتی پر هزینه مانند ماینینگ، رمزنگاری و هش‌کردن برای تأمین امنیت دارد. علاوه بر این، گره‌ها باید دفتر کل را همگام‌سازی کنند که نیاز به پهنای باند و فضای ذخیره‌سازی بالا دارد [42]. به دلیل رفتار متحرک و متنوع اینترنت اشیا زیرآبی [43]، پروتکل مسیریابی استاتیک نامناسب است به دلیل نیاز به منابع اضافی. نویسندگان پروتکل مسیریابی واکنشی را پیشنهاد می‌کنند که از نظر استفاده از انرژی در یک شبکه بزرگ ناکارآمد است [44]. علاوه بر این، بلاکچین نیاز به اتصال دائم با بلاکچین دارد که در محیط متحرک امکان‌پذیر نیست [45]، [46]. همچنین، مشتریان سبک به نرخ بالای داده‌های downlink نیاز دارند، زیرا باید با دفتر کل همگام‌سازی شوند [47].

2-4-2- روش‌ها

نویسندگان مکانیزم‌های چندگانه هم‌افزا را برای افزایش سازگاری بین دستگاه‌های فروشندگان مختلف پیشنهاد می‌کنند [42]. سطح قابل تحمل از دشواری به ظرفیت هر گره بستگی دارد تا برای شرکت در مکانیزم اجماع به صورت برابر باشد. مکانیزم تخلیه ذخیره‌سازی برای مقابله با تراکنش‌های نامربوط پیشنهاد شده است. یک زنجیره سبک (lightchain) توسعه داده شده که کمک می‌کند از تداخل اطلاعات جلوگیری شود. نویسندگان در [44] پروتکل مسیریابی سبک را برای رفع محدودیت مسیریابی ناکارآمد پیشنهاد می‌کنند. در اینجا، پیام‌های hello و کنترل کاهش یافته‌اند. فیلتر بلوم برای حفظ حریم خصوصی استفاده می‌شود که در آن نام مستعار برای گره‌ها فراهم می‌شود تا به صورت ناشناس در شبکه شرکت کنند. بلاکچین برای ذخیره امن داده‌ها استفاده می‌شود. نویسندگان در [45] ایده‌ای برای ذخیره‌سازی کارآمد داده‌ها پیشنهاد می‌کنند. تعداد محدودی از بلوک‌ها بر اساس توانایی هر گره تولید می‌شود. همچنین، بلوک‌های N-1 حذف می‌شوند و تنها آخرین بلوک در بلاکچین متحرک نگهداری می‌شود تا مسئله ذخیره‌سازی حل شود. محاسبات لبه سیار مبتنی بر چارچوب بلاکچین برای ماینینگ و ذخیره‌سازی محتوای داده‌های گره‌ها در [46] پیشنهاد شده است. برای خلاص شدن از تخلیه ذخیره‌سازی داده‌ها، نقاط دسترسی و کاربران نزدیک برای به اشتراک‌گذاری داده‌ها در نظر گرفته می‌شوند. نویسندگان در [47] طرح تجمیع داده برای افزایش عمر شبکه و کارآیی ذخیره‌سازی بلاکچین پیشنهاد می‌کنند، در حالی که دستگاه‌های سبک IoT سر اطلاعات را حمل می‌کنند و مقدار واقعی را از طریق درخت مرکل پاتریشیا پیدا می‌کنند، که از طریق اثبات شمول نگهداری می‌شود.

2-5- مکانیزم‌های ذخیره‌سازی برای گره‌های WSN

2-5-1- مشکلات

کمبود فضای ذخیره‌سازی گره‌های حسگر و اعتماد بین خریدار و فروشنده در هنگام معامله، دو مشکل اصلی در WSNها هستند [48]. علاوه بر این، نرخ به‌روزرسانی کند برای همگام‌سازی دفتر کل بر مقیاس‌پذیری تأثیر می‌گذارد. تانگل برای رفع مشکل مذکور پیشنهاد شده است. با این حال، هنوز مشکل نرخ بالای تولید اطلاعات را دارد. همچنین، گره‌های IoT به باتری‌های بیشتر و پهنای باند برای اعتبارسنجی تراکنش و ارتباطات نیاز دارند [49]. داده‌ها به ایستگاه‌های پایه برای پردازش داده‌ها مانند تجمیع ارسال می‌شوند، که در یک پایگاه داده مرکزی ذخیره می‌شود که ممکن است در معرض نقطه ضعف واحد قرار گیرد [50].

2-5-2- روش‌ها

نویسندگان در [48] یک مدل مبتنی بر انگیزه برای ذخیره داده‌ها در IPFS پیشنهاد می‌کنند. انگیزه‌ای برای IPFS برای ذخیره حجم زیادی از داده‌ها فراهم می‌شود. یک طرح رمزنگاری نامتقارن استفاده می‌شود. یک قرارداد هوشمند برای فرستنده و خریدار نوشته می‌شود تا شخص ثالث حذف شود. بلاکچین و IOTA دو فناوری توزیع‌شده و غیرمتمرکز هستند که در زمینه‌های مختلف مورد بررسی قرار گرفته‌اند. هر دو فناوری مشکل نرخ تولید اطلاعات را دارند که بر عملکرد شبکه تأثیر می‌گذارد. نویسندگان در [49] مفهوم سن اطلاعات را پیشنهاد می‌کنند که ترافیک در شبکه را کنترل می‌کند.

3- مدل سیستم

این بخش مکانیزم LRA را پیشنهاد می‌کند که از مسیریابی SDN فعال شده با GA پشتیبانی می‌کند. ما سناریوهای مختلفی با تعداد متغیر شبکه‌های IoT (خوشه‌ها) برای بررسی مقیاس‌پذیری سیستم خود در نظر گرفته‌ایم، همان‌طور که در شکل (1) نشان داده شده است. علاوه بر این، پس از محاسبه مسیر، گره‌های مخرب یا مرده در مرحله انتقال بسته شناسایی می‌شوند. همچنین، بلاکچین برای ذخیره شناسه‌های گره‌های مخرب استفاده می‌شود. محدودیت‌های شناسایی شده (در بخش 1 مورد بحث قرار گرفته‌اند)، راه‌حل‌های پیشنهادی و اعتبارسنجی آن‌ها در جدول (2) نشان داده شده‌اند.

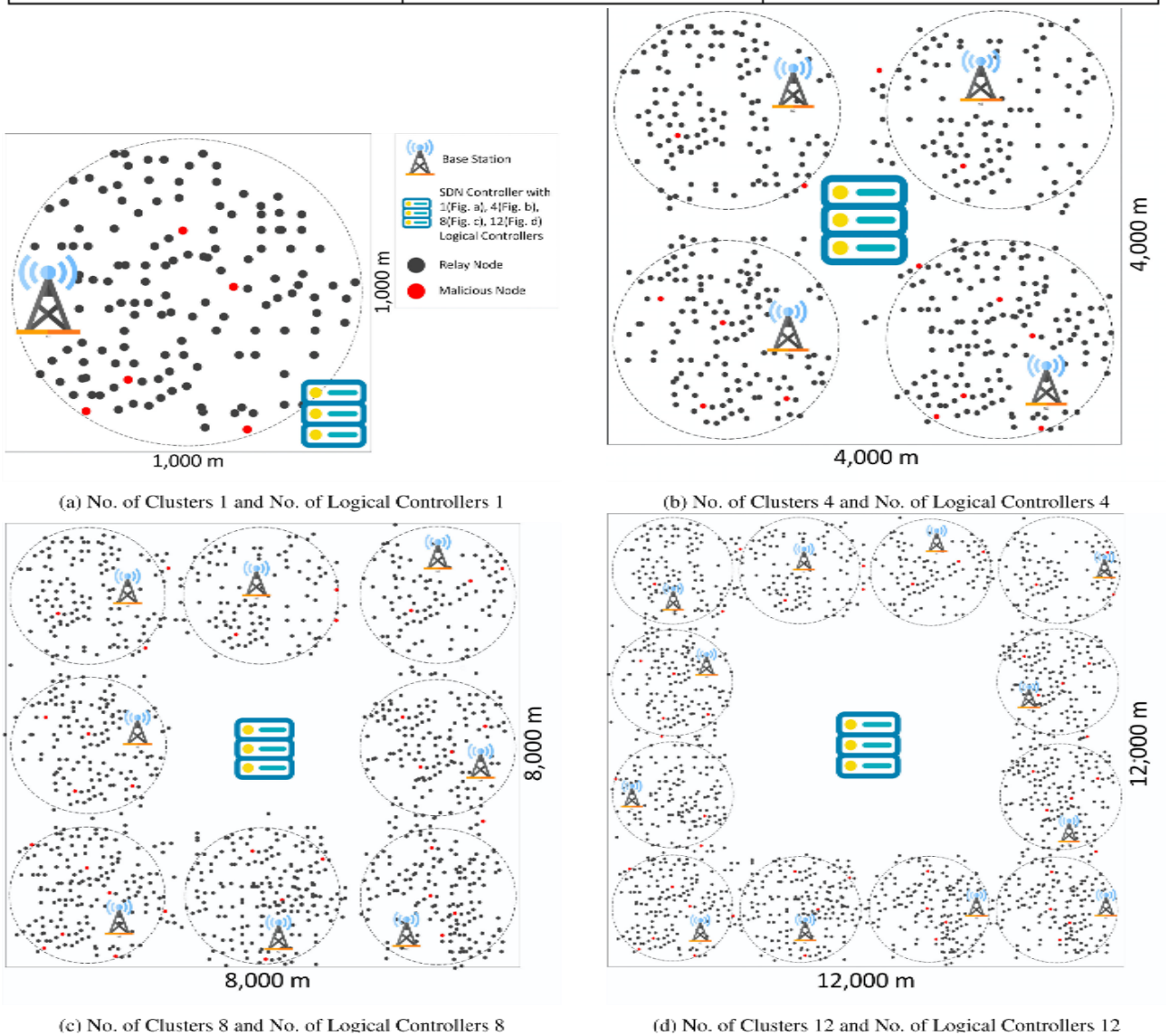
3-1- مفروضات و مدل شبکه

مکانیزم‌های احراز هویت و مسیریابی بر اساس برخی مفروضات پایه‌ای که برای تحقق نیازهای شبکه ضروری هستند، پیشنهاد می‌شوند. مفروضات شبکه به شرح زیر هستند:

- تمامی ایستگاه‌های پایه امن بوده و منابع کافی برای استقرار بلاکچین دارند،
- کنترلر SDN به عنوان یک نهاد مورد اعتماد در شبکه در نظر گرفته می‌شود،
- گره‌های RN به عنوان ایستا در نظر گرفته شده و فاصله آن‌ها از یکدیگر ثابت می‌ماند،
- فرض بر این است که گره‌های عادی داده‌های معتبر را به RN ارسال می‌کنند و
- گره‌های مخرب و مرده به صورت متقابل استفاده می‌شوند و تنها گره‌های مخرب می‌توانند حمله سیاهچاله انجام دهند.

جدول (1) : نقشه برداری از محدودیت ها، راه حل های پیشنهادی و اعتبار سنجی آنها

Identified Limitations	Proposed Solutions	Validations
L1: Authentication of nodes using group signature could be harmful [14]	S1: Lightweight authentication of RNs using blockchain	V1: Execution and transaction costs over blockchain (6a, 6b)
L2: Inefficient energy consumption [16]	S2: GA enabled SDN controller to find the optimized route	V2: Energy consumption (7a)
L3: No mechanism for the detection of malicious RNs [15]	S3: Acknowledgment mechanism	V3: Number of malicious nodes and packets dropped (7b)



(a) No. of Clusters 1 and No. of Logical Controllers 1

(b) No. of Clusters 4 and No. of Logical Controllers 4

(c) No. of Clusters 8 and No. of Logical Controllers 8

(d) No. of Clusters 12 and No. of Logical Controllers 12

FIGURE 1. **Different scenarios for proposed model.**

2-3- توضیحات سیستم

این زیربخش جریان کاری مدل سیستم را که در شکل (2) نشان داده شده است، ارائه می‌دهد.

- مرحله 1: گره‌های RN درخواست‌های ثبت‌نام را برای ثبت خود در بلاکچین تولید می‌کنند.
- مرحله 2: RNها توسط بلاکچین احراز هویت می‌شوند تا بخشی از شبکه شوند.
- مرحله 3: گره مبدا که داده‌ای برای ارسال دارد، درخواست مسیریابی را به بلاکچین ارسال می‌کند.
- مرحله 4: بلاکچین درخواست را به کنترلر SDN فعال شده با GA ارسال می‌کند.
- مرحله 5: مسیری که توسط کنترلر SDN محاسبه شده است به بلاکچین ارسال می‌شود. RCM مسیر را با استفاده از لیست گره‌های مخرب (MNL) که قبلاً توسط مکانیزم MND در بلاکچین نگهداری می‌شود، تأیید می‌کند، همان‌طور که در زیربخش (3-7) ذکر شده است.

- مرحله 6: اگر مسیر صحیح باشد، به گره درخواست‌دهنده (مبدا) در شبکه ارسال می‌شود.
- مرحله 7: گره درخواست‌دهنده مسیر را دریافت کرده و با استفاده از مکانیزم تأیید، گره‌های مخرب را شناسایی می‌کند. اگر هیچ RN بسته تأیید را برنگرداند، گره مبدا بسته را پنج بار مجدداً ارسال می‌کند. اگر هیچ تأییدی دریافت نشود، گره مبدا RN را به عنوان مخرب اعلام می‌کند.
- مرحله 8: شناسه گره مخرب شناسایی شده به MNL اضافه می‌شود که توسط RCM استفاده می‌شود. سپس، مرحله 4 دوباره آغاز می‌شود.

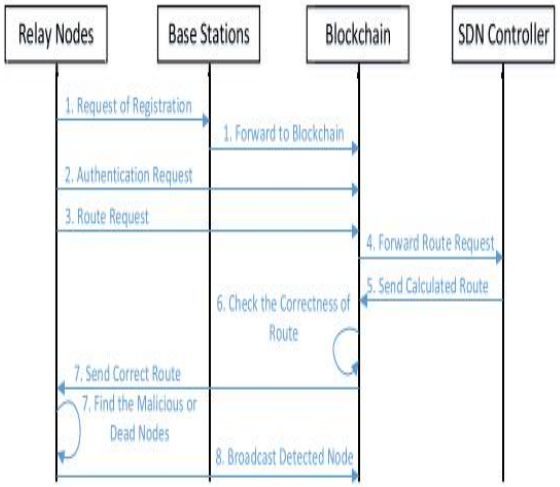


FIGURE 2. Workflow of the proposed model.

3-3- عملکرد بلاکچین

بلاکچین بر روی ایستگاه‌های پایه (BSs) پیاده‌سازی شده است تا به صورت امن مدارک شناسایی گره‌ها را ذخیره کند. بلاکچین همچنین برای احراز هویت گره‌ها در مکانیزم LRA و اعتبارسنجی مسیر در مکانیزم RCM استفاده می‌شود. در ابتدا، گره‌ها از طریق یک قرارداد هوشمند در بلاکچین ثبت‌نام می‌شوند. سپس یک تراکنش انجام شده و توسط گره‌های ماینر با استفاده از الگوریتم اجماع PoW اعتبارسنجی می‌شود. در نهایت، دفتر کل با همه ایستگاه‌های پایه در شبکه بلاکچین به اشتراک گذاشته می‌شود و پس از اجرای اجماع، تراکنش به بلوک اضافه می‌شود. الگوریتم‌های اجماع زیادی برای توسعه اجماع بین موجودیت‌های توزیع شده و ناشناس استفاده می‌شوند، مانند PoW، PoS، PoA (Proof of Authority) و غیره. در مدل ما، مکانیزم اجماع PoW برای اطمینان از اعتماد در شبکه استفاده می‌شود. در PoW، گره‌های ماینر مختلف با یکدیگر در حل پازل رقابت می‌کنند. گره ماینری که پازل را اول حل کند، مسئول اعتبارسنجی تراکنش‌ها و افزودن بلوک‌ها به بلاکچین می‌شود. با این حال، PoW نیاز به منابع محاسباتی بالایی برای حل پازل و افزودن تراکنش به بلاکچین دارد. ایستگاه‌های پایه هیچ محدودیتی ندارند، بنابراین PoW برای فرآیند ماینینگ استفاده می‌شود. علاوه بر این، بلاکچین برای رفع مشکل نقطه شکست واحد (single point of failure) استفاده می‌شود. همچنین، مشکل تنگنای پهنای باند مکانیزم‌های متمرکز را جلوگیری می‌کند. بلاکچین در برابر تغییرات مقاوم است و شبکه را از حملات مختلفی مانند حمله سیبل، حمله جعل هویت و غیره محافظت می‌کند. عملکرد بلاکچین در شکل (3) قابل مشاهده است.

4-3- احراز هویت گره‌های رله

فرآیندهای ثبت‌نام و احراز هویت در الگوریتم (1) بحث شده‌اند. احراز هویت گره‌های ارسال‌کننده (forwarding nodes) ضروری است، همان‌طور که در بخش 1 مورد بحث قرار گرفت. در این مقاله، مکانیزم LRA را برای ذخیره مدارک شناسایی گره‌ها در بلاکچین پیشنهاد می‌کنیم. احراز هویت گره‌ها قبل از شروع ارتباط انجام می‌شود، که شبکه را در مرحله اولیه از گره‌های غیرمجاز محافظت می‌کند. فرمول (1) پارامترهای مربوط به درخواست ثبت‌نام یک گره را ترکیب می‌کند.

$$Reg_{req} = (ID_{RN}, L_{RN}, En_{RN}). \quad (1)$$

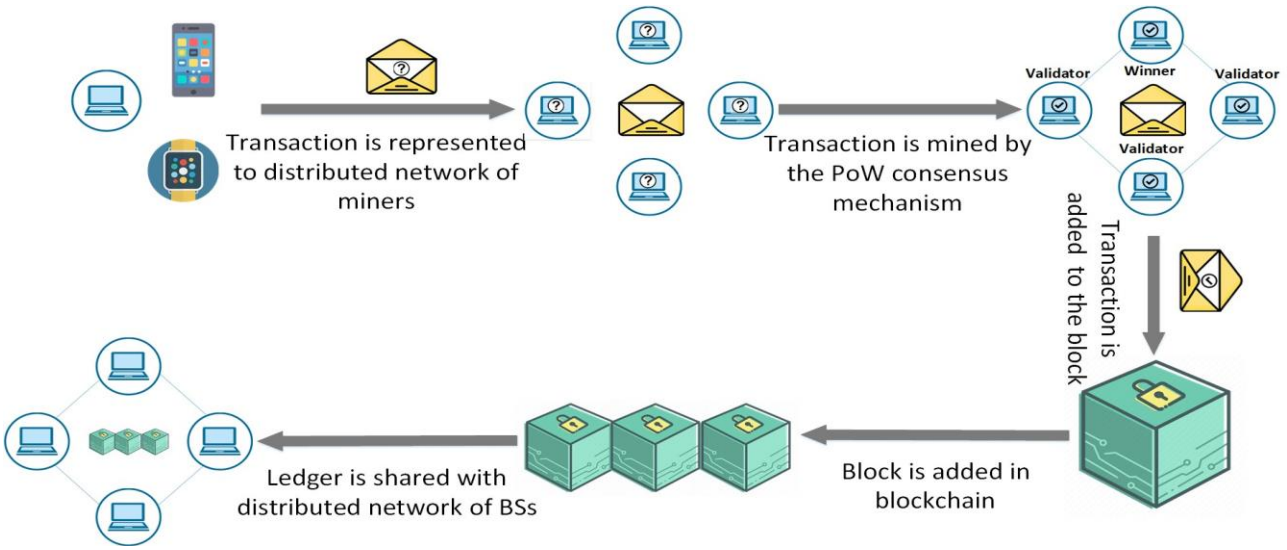
که در آن، ID_{RN}، L_{RN} و En_{RN} به ترتیب نماینده شناسه، مکان و انرژی گره رله (RN) هستند. اگر مدارک شناسایی قبلاً وجود داشته باشند، انرژی باقی‌مانده گره به‌روزرسانی می‌شود. در غیر این صورت، بلاکچین ID_{RN}، L_{RN} و En_{RN} را ذخیره می‌کند. قبل از ثبت‌نام، اگر انرژی گره کمتر از حد مشخصی باشد، آن رد می‌شود؛ در غیر این صورت، در شبکه ثبت‌نام می‌شود. پس از آن، احراز هویت گره‌ها با مقایسه شناسه‌های آن‌ها با شناسه‌های ذخیره‌شده در بلاکچین انجام می‌شود. علاوه بر این، مکان‌های گره‌ها با مکان‌های ذخیره‌شده مقایسه می‌شوند، که باید یکسان باشند زیرا گره‌ها ثابت هستند، طبق الگوریتم (1).

Algorithm 1: LRA for Forwarding Nodes

```
Inputs: ID_RN, L_RN, En_RN;
Outputs: Message;
Send to BS: ID_RN, L_RN, En_RN;
if ID_RN, L_RN Not Stored in Blockchain then
    if En_RN ≥ threshold then
        Store ID_RN, L_RN, En_RN;
        return Accepted;
    else
        return Rejected;
    end
else
    Update En_RN;
    return Updated;
end
```

5-3- مسیریابی SDN فعال شده با GA

SDN یک فناوری متمرکز است که برای کشف مسیر استفاده می‌شود. همچنین برای پیاده‌سازی سیاست‌های مختلف که قسمت‌های دیگر شبکه را کنترل می‌کنند، به کار می‌رود. SDN از دو صفحه تشکیل شده است: صفحه داده و صفحه کنترل. صفحه داده تنها داده را بر اساس سیاست یا مسیر تعریف شده توسط کنترلر SDN به گام بعدی ارسال می‌کند. در مقابل، صفحه کنترل سیاست‌ها یا مسیرهایی برای ارسال داده تعریف می‌کند. مسیرها یا سیاست‌های تعریف شده بر روی صفحه داده پیاده‌سازی می‌شوند تا ارتباط کارآمد بین گره‌ها را تضمین کنند. در سناریوی ما، SDN برای محاسبه مسیرهای با بهره‌وری انرژی در یک شبکه IoT استفاده می‌شود، با استفاده از



شکل (3) : عملکرد بلاک چین

TABLE 3. Mapping of GA and IoT network's terminologies.

GA's Terminologies	IoT Network's Terminologies
Population	Set of Possible Routes
Chromosomes	Routes
Gene	Hop
Off-spring	Newly Generated Route
Parents	Selected Routes for Crossover

یک نهاد متمرکز. بنابراین، انرژی گره‌های رله (RNs) حفظ می‌شود زیرا خود RN مسیر را محاسبه نمی‌کند. علاوه بر این، کوتاه‌ترین و با بهره‌ورترین مسیر از طریق کنترلر SDN فعال شده با GA محاسبه می‌شود تا عمر شبکه افزایش یابد.

GA برای یافتن راه‌حل‌های بهینه برای مشکلات استفاده می‌شود. این الگوریتم با مجموعه اولیه‌ای از راه‌حل‌ها که جمعیت نامیده می‌شود، کار می‌کند. تناسب هر راه‌حل از طریق یک تابع تناسب محاسبه می‌شود. سپس دو راه‌حل والدین برای انجام تقاطع و جهش انتخاب می‌شوند. در تقاطع، انتهای والدین انتخاب شده در یک نقطه انتخاب شده تبادل می‌شوند تا دو فرزند جدید ایجاد شوند که دارای ویژگی‌های هر دو والدین هستند. این نقطه از ژن انتخاب می‌شود، جایی که هر دو والدین مقدار یکسان دارند. این به این دلیل است که در ارتباطات بی‌سیم، گره‌ها باید در محدوده ارتباطی باشند، در حالی که پس از تقاطع، احتمال حضور گره‌ها فراتر از محدوده ارتباطی وجود دارد. علاوه بر این، فرزندان با استفاده از فرآیند جهش اصلاح می‌شوند، که یک ژن را معکوس می‌کند. سپس تناسب فرزندان جدید محاسبه می‌شود. اگر تناسب بهتر از تناسب والدین باشد، فرزندان والدین را جایگزین می‌کنند، در غیر این صورت، آن‌ها دور انداخته می‌شوند. تمام مراحل در شکل (4) نشان داده شده است. اصطلاحات GA و شبکه IoT در جدول (3) نقشه‌برداری شده‌اند و در مقاله به صورت متناوب استفاده می‌شوند.

3-5-1- جمعیت اولیه

در مدل پیشنهادی، گره‌های رله (RNs) بر اساس فاصله آن‌ها از گره قبلی (گره مبدا یا گره میانی) انتخاب شده و به لیست ارسال‌کننده اضافه می‌شوند. از این لیست برای به دست آوردن مسیر بهینه از گره مبدا به گره مقصد استفاده می‌شود. به طور مشابه، هر مسیر ممکن از طریق فاصله محاسبه شده پیدا می‌شود، به عنوان مثال، برای نه گره، یک زیرشبکه در شکل a5 نشان داده شده است و مسیرهای ممکن از گره مبدا به گره مقصد در شکل b5 نمایش داده شده‌اند. معمولاً در GA، جمعیت اولیه به صورت تصادفی تولید می‌شود، اما این احتمال وجود دارد که گره‌ای در مسیر در لیست همسایگان گره قبلی وجود نداشته باشد. این افزودن تصادفی در مسیر شبکه را گمراه کرده و منابع اضافی مصرف می‌کند. بنابراین، ما فاصله هر گره از گره‌های دیگر را محاسبه کرده و لیست همسایگان را بر اساس محدوده ارتباطی حفظ می‌کنیم.

3-5-2- تابع تناسب و انتخاب والدین

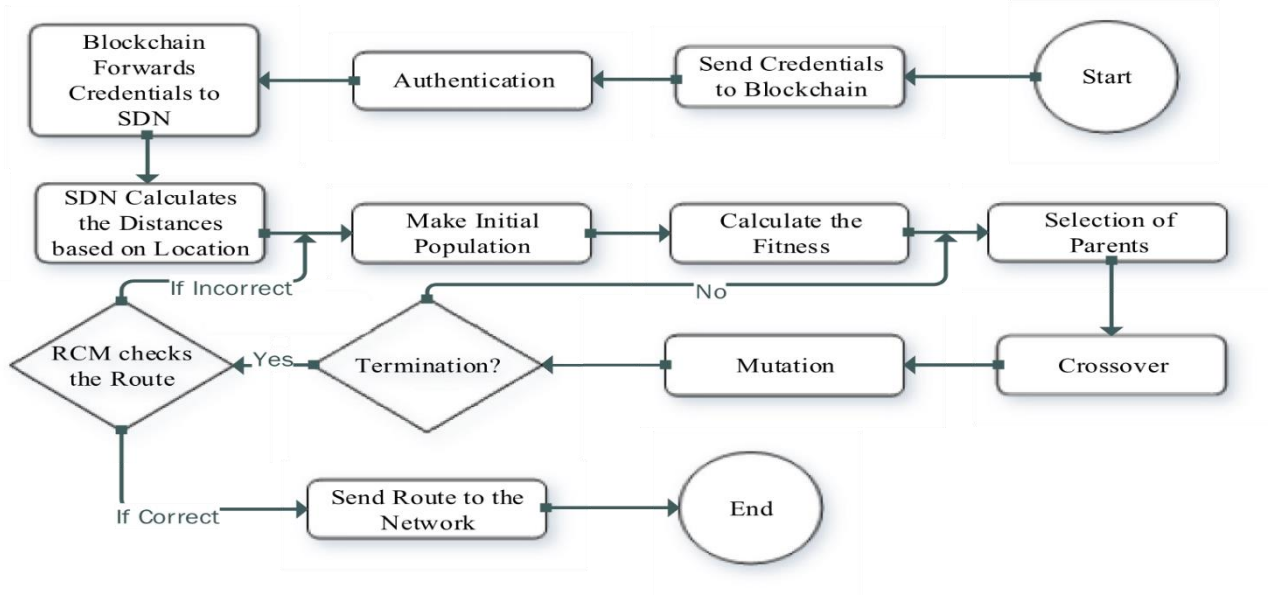
تابع تناسب برای محاسبه مقدار تناسب هر مسیر بر اساس هدف استفاده می‌شود. تمام مسیرها بر اساس مقادیر تناسب مرتب می‌شوند. هدف، کمینه کردن فاصله کل بین مبدا و مقصد است. اگر فاصله کل مسیر کوچک باشد، مقدار تناسب بزرگ خواهد بود. مقدار تناسب بر اساس [52] محاسبه می‌شود.

$$Fitness(k) = \frac{1}{\sum_{i=0}^{N-1} Dist(C_i, Crom(k, i+1))}. \quad (2)$$

که در آن Fitness(k) نشان دهنده تناسب مسیر k_{th} است، در حالی که Crom(k,i + 1) نشان دهنده گام بعدی $hop\ i_{th}$ در مسیر k_{th} است. علاوه بر این، Dist نمایانگر فاصله بین گره‌ها است و C_i نشان دهنده گام فعلی در کروموزوم انتخاب شده است.

3-5-3- تقاطع و جهش

برای ساختن مسیرها بر اساس هدف، یک تقاطع یک نقطه‌ای انجام می‌شود. تقاطع با انتخاب یک نقطه مشترک در هر دو مسیر یا حداقل یک همسایه مشترک، تنوع بیشتری در فرزندان ایجاد می‌کند. به عبارت دیگر، لبه‌ها برای



شکل (4) : نمودار جریان برای مکانیسم مسیریابی SDN فعال GA.

تشکیل مسیر جدید برای تنوع بیشتر جمعیت تعویض می‌شوند. اگر تناسب مسیرهای فرزندان بهتر از مسیرهای موجود باشد، مسیرهای قبلی جایگزین می‌شوند، در غیر این صورت، فرزندان دور انداخته می‌شوند. علاوه بر این، در GA، جهش به طور تصادفی در ژن انتخاب شده انجام می‌شود. در حالی که، در مورد ما، جهش زمانی انجام می‌شود که گره‌ای با انرژی کم یا فاصله زیاد وجود داشته باشد. گام انتخاب شده با برخی گره‌های دیگر از لیست همسایگان جایگزین می‌شود. تناسب دوباره محاسبه می‌شود و اگر مقدار نتیجه بهتر از قبل باشد، مسیرهای جدید جایگزین مسیرهای قبلی می‌شوند.

6-3- مکانیزم صحت مسیر

مکانیزم RCM برای مسیریابی مبتنی بر هیوریستیک ضروری است زیرا جمعیت در هر تکرار در تکنیک‌های هیوریستیکی مانند GA به‌روزرسانی می‌شود. بنابراین، مسیر بهینه نهایی ممکن است شامل گره‌های مخرب یا مرده باشد که مصرف انرژی را در حین ارسال بسته‌ها افزایش می‌دهد. در بلاکچین، لیست گره‌های مخرب (MNL) توسط شبکه IoT نگهداری می‌شود. مکانیزم تشخیص گره‌های مخرب یا مرده در بخش (3-7) توضیح داده شده است. مکانیزم RCM به مسیر نتیجه نگاه می‌کند و شناسه هر گره را با MNL که در بلاکچین نگهداری می‌شود، مقایسه می‌کند. اگر شناسه یک گره در MNL یافت شود، بلاکچین درخواست محاسبه مجدد مسیر را از کنترلر SDN مطابق با الگوریتم (2) می‌دهد.

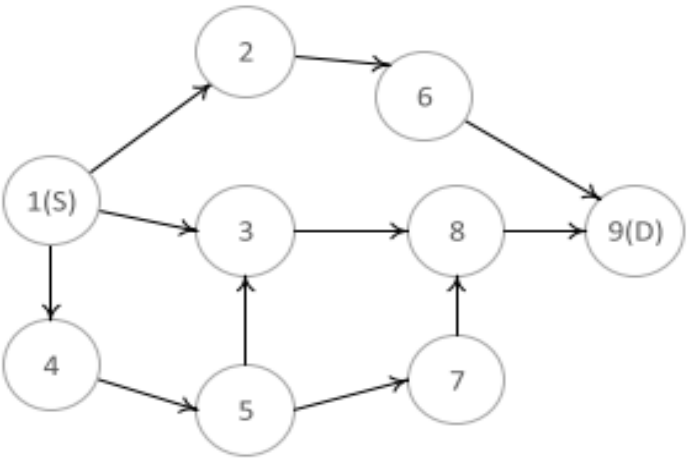
7-3- مکانیزم تشخیص گره مخرب

تعداد دستگاه‌های IoT روز به روز در حال افزایش است. بنابراین، احتمال ورود غیرمجاز گره‌ها وجود دارد که بر عملکرد کلی شبکه تأثیر می‌گذارد. برای رسیدگی به این مسئله، مکانیزم LRA را برای احراز هویت گره‌ها پیشنهاد می‌کنیم. با این حال، گره‌های مخرب ممکن است حتی پس از احراز هویت در شبکه وجود داشته باشند زیرا یک گره می‌تواند توسط یک مهاجم به خطر بیفتد. علاوه بر این، گره‌ها ممکن است به دلیل تخلیه سریع انرژی خود مرده

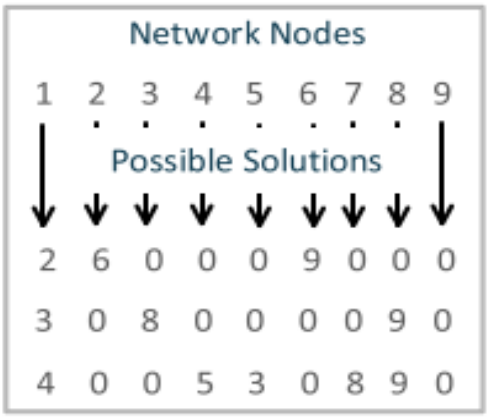
Algorithm 2: Route Correctness Mechanism

```
1  Inputs: Route, MNL;
2  Outputs: Message;
3  for i ← 1 to Number of Hops in Route do
4      if Hop not exists in MNL then
5          Send Route to Network;
6          return Correct;
7      else
8          Re-calculation Request;
9          return Incorrect;
10     end
11 end
```

باشند. این دو نوع گره باعث مصرف اضافی انرژی به دلیل افت بسته‌ها به دلیل ارسال مجدد می‌شوند. برای تشخیص گره مخرب، گره مبدا بسته سلام (hello packet) را به گام بعدی در مسیر محاسبه شده قبل از شروع ارتباط ارسال می‌کند. اگر گام بعدی زنده و قانونی باشد، مدارک خود را در بسته تاییدیه (acknowledgment packet) اضافه کرده و آن را به گره مبدا ارسال می‌کند مطابق با الگوریتم 3. به طور همزمان، گره گیرنده بسته سلام را برای بررسی زنده بودن گام بعدی خود ارسال می‌کند و این روند ادامه دارد. اگر هیچ یک از گره‌ها تاییدیه را ارسال نکند، بسته سلام پنج بار دیگر با همان شرایط ارسال می‌شود. اگر تاییدیه دریافت شود، گره مبدا ارتباط را آغاز می‌کند، در غیر این صورت، گره به عنوان مخرب یا مرده اعلام می‌شود. شناسه گره مخرب یا مرده به بلاکچین ارسال می‌شود. بلاکچین مدارک گره مخرب را حذف کرده و شناسه آن را به MNL اضافه می‌کند، همان‌طور که در بخش (6-3) بحث شد. علاوه بر این، این روش گره‌های مخرب یا مرده را به روشی بسیار ساده تشخیص می‌دهد، بنابراین طول عمر گره‌ها را به دلیل مصرف کمتر انرژی افزایش می‌دهد. بسته سلام بسیار سبک است و مصرف انرژی کمی دارد. علاوه بر این، نگهداری MNL نیز انرژی را ذخیره می‌کند زیرا در تشخیص گره‌های مخرب در مسیر محاسبه شده در مراحل اولیه کمک می‌کند.



(a)



(b)

FIGURE 5. **(a) Sub-network architecture (b) Possible routes.**

• تنها مسیر صحیح به گره منبع ارسال می‌شود تا منابع شبکه حفظ شود.

• گره‌های مخرب اعلام شده دیگر اجازه مشارکت در شبکه را نخواهند داشت.

TABLE 4. **Simulation parameters.**

Parameters	Values
Sensing Area	$1000m^2$- $12000m^2$
No. of RNs	1000-12000
No. of BSs	12
Wireless Range of RNs	250 m
Initial Energy for RNs	0.5J
Initial Energy for BSs	No. Energy Constraint
Network Topology	Random Distribution

Algorithm 3: Malicious Nodes' Detection

```
Inputs: Route;
Outputs: Message;
Send hello Packet;
for i ← 1 to 5 do
    if Acknowledgement Packet Received then
        Send Packet to route's Next Hop;
        return Route is Correct;
        break;
    else
        Send hello Packet Again;
        if i == 5 then
            return ID of Malicious Node;
        end
    end
end
```

4- ارزیابی عملکرد

در این بخش، ارزیابی عملکرد مدل پیشنهادی و روش‌های آزمایش مورد بحث قرار می‌گیرد.

4-1- محیط شبیه‌سازی

ما محیط بلاکچین را با استفاده از MetaMask، Ganache و Remix IDE بر روی ویندوز 10 پرو، پردازنده 64 بیتی اینتل Core m3 با سرعت 1.61 گیگاهرتز و 8 گیگابایت رم راه‌اندازی کردیم. قرارداد هوشمند به زبان Solidity نوشته شده است. تمامی پارامترهای شبیه‌سازی با سناریوهای مختلف در جدول 4 لیست شده‌اند.

4-2- شرایط مدل پیشنهادی

• اگر هیچ RN بسته تاییدیه را ارسال نکند، گره منبع پنج بار دیگر بسته را ارسال می‌کند. اگر تاییدیه‌ای دریافت نشود، گره منبع RN را به عنوان مخرب اعلام می‌کند.

• تنها BSها مسئول احراز هویت گره‌های عادی هستند زیرا بلاکچین بر روی BSها پیاده‌سازی شده است.

• تمامی گره‌ها باید به بسته سلام گره منبع پاسخ دهند.

4-3- اعتبارسنجی

در این بخش، شبیه‌سازی‌های مدل پیشنهادی را با در نظر گرفتن مصرف گاز، انرژی باقی‌مانده شبکه و تعداد بسته‌های از دست رفته انجام داده‌ایم. مراحل تجربی مدل ما به شرح زیر است:

• مرحله 1: احراز هویت

• مرحله 2: محاسبه مسیر

• مرحله 3: تشخیص گره مخرب

4-3-1- احراز هویت

در این بخش، عملکرد و اثربخشی مدل ما با استفاده از مصرف گاز مکانیزم LRA ارزیابی شده و با طرح HBA موجود مقایسه شده است. مصرف گاز در محیط بلاکچین یک واحد اساسی برای محاسبه هزینه تراکنش و اجرا است. هزینه استقرار شامل هزینه‌های تراکنش و محاسباتی است که توسط فراخوان قرارداد هوشمند پرداخت می‌شود. هزینه تراکنش برای افزودن یک تراکنش به بلاکچین پرداخت می‌شود، در حالی که هزینه اجرا برای انجام عملیات مختلف در قرارداد هوشمند پرداخت می‌شود. هزینه محاسباتی مکانیزم LRA پیشنهادی ما در شکل (6-b) و جدول (5) نشان داده شده است. تکنیک موجود اندازه پیام بزرگتری دارد و بنابراین باعث مصرف گاز بیشتری نسبت به مکانیزم LRA پیشنهادی می‌شود. اندازه پیام در تکنیک موجود بزرگتر است

زیرا پارامترهای زیادی در مکانیزم احراز هویت شرکت دارند. از سوی دیگر، LRA شامل پارامترهای کمتری است که نیاز به ذخیره شدن دارند. علاوه بر این، مجموعه اول از نوارها هزینه استقرار را نشان می‌دهد که کارایی مدل پیشنهادی را از نظر مصرف گاز نشان می‌دهد. به همین ترتیب، مجموعه‌های دوم و سوم نوارها کارایی ثبت‌نام و احراز هویت را به ترتیب نشان می‌دهند. هزینه ثبت‌نام بیشتر از هزینه احراز هویت است زیرا مدارک در زمان ثبت‌نام باید در بلاکچین ذخیره شوند که هزینه بیشتری نیاز دارد. در احراز هویت، مدارک فقط باید با مدارک ذخیره‌شده مقایسه شوند. بنابراین، فرآیند احراز هویت نیاز به گاز کمتری نسبت به فرآیند ثبت‌نام دارد. به همین ترتیب، دلایل مشابهی برای هزینه تراکنش که در شکل (7-a) و جدول (5) نمایش داده شده‌اند، اعمال می‌شود.

TABLE 5. Gas consumption.

Cost Name	Scheme	C1	C2	C3
Transaction Cost	HBA	405984	188497	58671
	LRA	302988	128111	48373
Execution Cost	HBA	265312	166073	72074
	LRA	201385	106455	62013

Note: C1 denotes Deployment, C2 denotes Registration and C3 denotes Authentication.

4-3-2- محاسبه مسیر

روش مسیریابی مبتنی بر SDN با GA با محاسبه انرژی باقی‌مانده شبکه پس از تشخیص گره مخرب جدید ارزیابی می‌شود. کاهش جزئی در کل انرژی پس از تشخیص گره مخرب جدید مشاهده می‌شود، همانطور که در شکل (7-a) نشان داده شده است. در سناریوی ما، در ابتدا چهار حالت که در بخش (4-4) ذکر شده‌اند، شبیه‌سازی می‌شوند. سپس بلاکچین برای نگهداری سوابق مدارک گره‌ها و اطمینان از صحت مسیر ادغام می‌شود. پس از این، حالات با افزایش تعداد گره‌ها، خوشه‌ها و کنترل‌کننده‌های منطقی SDN اجرا می‌شوند. این حالات شامل 1، 4، 8 و 12 کنترل‌کننده منطقی SDN برای 1، 4، 8 و 12 خوشه به ترتیب هستند. آنها برای بررسی مقیاس‌پذیری مدل پیشنهادی اجرا می‌شوند. هر مجموعه نوارها در شکل (7-a) چهار حالت مذکور را نشان می‌دهد. می‌توانیم ببینیم که در هر حالت، انرژی مصرف شده به طور منطقی افزایش می‌یابد، زیرا تعداد گره‌ها و خوشه‌ها افزایش می‌یابد. بنابراین، هیچ اضافه باری از مصرف انرژی وجود ندارد. مصرف انرژی کلی شبکه حداقل است زیرا مسیر جدید پس از تشخیص گره‌های مخرب محاسبه می‌شود. مسیر جدید نرخ افت بسته‌ها را کاهش می‌دهد که بر مصرف انرژی گره‌ها تأثیر می‌گذارد. همچنین، تعداد بسته‌های ارسالی موفق افزایش می‌یابد که برای یک شبکه کارآمد ضروری است. بنابراین، استفاده از منابع بر روی بسته‌های ارسال شده در نظر گرفته نمی‌شود. مصرف حداقل انرژی در هر تشخیص جدید نشان‌دهنده دستیابی به هدف کار ما است. علاوه بر این، این آزمایشات برای چهار حالت قبلی به منظور ارزیابی مقیاس‌پذیری مدل پیشنهادی انجام شده‌اند. علاوه بر این، مصرف انرژی به طور منطقی با افزایش اندازه شبکه افزایش می‌یابد، همانطور که در شکل (7-a) نشان داده شده است. با این حال، مصرف انرژی از یک مقدار مورد انتظار بیشتر نمی‌شود. دلیل این است که تعداد پرش‌ها در مسیر محاسبه شده به دلیل انتخاب کوتاه‌ترین مسیر مبتنی بر GA و محاسبه مسیر از طریق کنترل‌کننده SDN متمرکز حداقل است. علاوه بر این، تخلیه انرژی گره‌های منبع و مقصد کمتر است زیرا آنها فقط باید بسته‌ها را ارسال یا دریافت کنند.

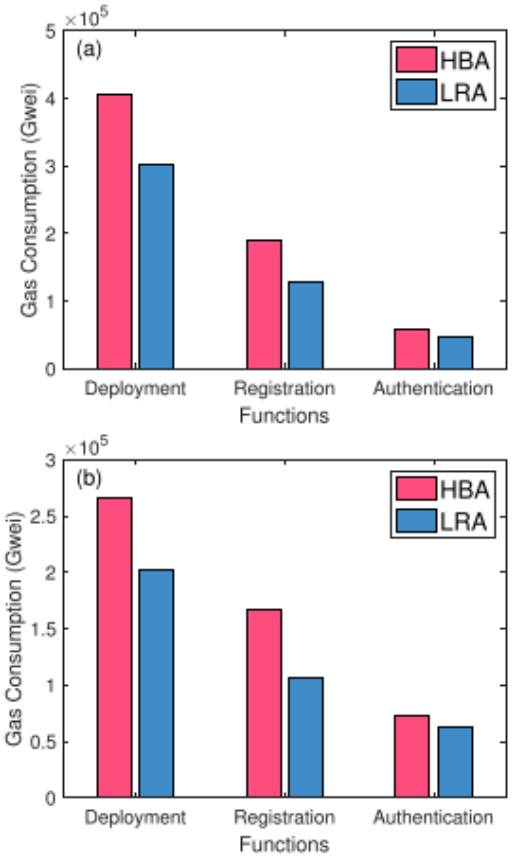


FIGURE 6. Gas Consumption in terms of (a) Transaction cost (b) Execution cost.

4-3-3- تشخیص گره مخرب

مسئله دیگری وجود دارد و آن وجود گره مخرب در گره‌های میانی است که بر ارتباط شبکه تأثیر می‌گذارد. علاوه بر این، مکانیزم MND با تعداد بسته‌های از دست رفته ارزیابی می‌شود. اگر هر گره‌ای مخرب یا مرده شود و این اطلاعات به شبکه پخش نشود، انرژی سایر گره‌ها به دلیل ارسال مجدد بسته‌ها ممکن است تمام شود. ما تعداد بسته‌های از دست رفته زمانی که هر گره مخرب تشخیص داده می‌شود را محاسبه کرده‌ایم. در شکل (7-b)، محور x تعداد گره‌های مخرب و محور y تعداد کل بسته‌های از دست رفته را نشان می‌دهد. در نهایت، تعداد بسته‌های از دست رفته به دلیل افزایش تعداد گره‌های مخرب افزایش می‌یابد. با این حال، تعداد بسته‌های از دست رفته به صورت تصاعدی افزایش نمی‌یابد زیرا گره‌های مخرب از طریق تایید پیام سلام سبک وزن شناسایی می‌شوند. این پیام‌های سلام بعد از یک بازه زمانی مشخص برای اطمینان از قابلیت اطمینان مسیر در طول عمر شبکه آغاز می‌شوند. شکل (7-b) رفتار نامطمئن را نشان می‌دهد زیرا تعداد متفاوتی از بسته‌ها در هر تکرار از دست می‌روند. تعداد بسته‌های از دست رفته به صورت افزایشی افزایش نمی‌یابد زیرا گره‌های مخرب در فواصل زمانی مختلف شناسایی می‌شوند. گاهی اوقات، گره‌های مخرب بلافاصله پس از تشخیص

TABLE 6. Time taken by different cases.

Cluster No.	No. of Clusters = 1 No. of Control Planes = 1	No. of Clusters = 4 No. of Control Planes = 4	No. of Clusters = 8 No. of Control Planes = 8	No. of Clusters = 12 No. of Control Planes = 12
1	0.780678	0.698778	0.707219	0.703964
2		0.768295	0.744087	0.736068
3		0.702707	0.714343	0.719232
4		0.807292	0.727246	0.742095
5			0.741775	0.720395
6			0.855588	0.782724
7			0.782842	0.722695
8			0.762140	0.717828
9				0.746192
10				0.821233
11				0.735601
12				0.724500
Average Time (sec)	**0.780678**	**0.744268**	**0.782842**	**0.679002**

آخرین شناسایی می‌شوند. این بدان معناست که مکانیزم شناسایی گره‌های مخرب را به طور موثر تشخیص می‌دهد. علاوه بر این، هنگامی که هر گره‌ای در مسیر مرده می‌شود، یک مسیر جدید توسط کنترل‌کننده SDN محاسبه می‌شود، بنابراین افت بسته‌ها کاهش می‌یابد که مصرف انرژی را کاهش داده و طول عمر کل شبکه را افزایش می‌دهد.

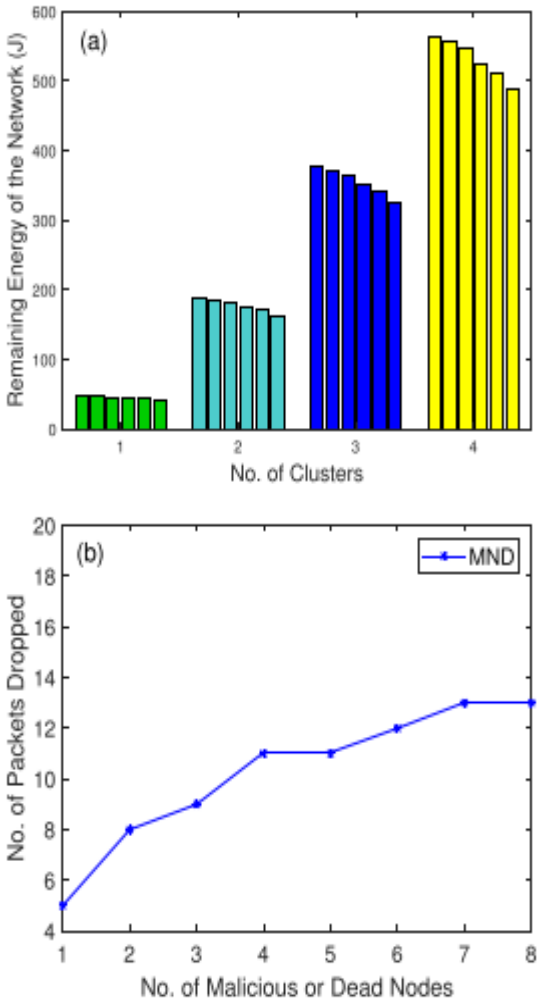


FIGURE 7. (a) Remaining energy of the networks (b) Number of packe dropped.

4-4- مطالعات موردی مدل پیشنهادی برای اعتبارسنجی مقیاس‌پذیری

برای شبیه‌سازی مدل پیشنهادی، تعداد مختلف خوشه‌ها و کنترل‌کننده‌های منطقی به شرح زیر در نظر گرفته شده‌اند:

- تعداد خوشه‌ها 1، تعداد کنترل‌کننده‌های منطقی 1
- تعداد خوشه‌ها 4، تعداد کنترل‌کننده‌های منطقی 4
- تعداد خوشه‌ها 8، تعداد کنترل‌کننده‌های منطقی 8
- تعداد خوشه‌ها 12، تعداد کنترل‌کننده‌های منطقی 12

در سناریوی ما، کنترل‌کننده SDN برای محاسبه مسیر برای دستگاه‌های IoT استفاده می‌شود و ممکن است بیش از یک کنترل‌کننده منطقی وجود داشته باشد. با این حال، شبیه‌سازی‌های ذکر شده در بالا برای بررسی مقیاس‌پذیری مدل پیشنهادی برای زمان محاسبه مسیر انجام شده‌اند. زمان متوسط تقریبا یکسان برای سناریوهای مختلف است، همانطور که در جدول 6 ذکر شده است. در جدول، ستون‌های 2، 3، 4 و 5 دارای یک، چهار، هشت و دوازده کنترل‌کننده منطقی هستند. از آنجایی که کنترل‌کننده‌های منطقی در صفحه کنترل SDN به صورت موازی کار می‌کنند، تفاوت زیادی بین زمان‌هایی که توسط کنترل‌کننده‌های منطقی گرفته می‌شود وجود ندارد. بنابراین، تأیید شده است که سیستم ما برای افزایش تعداد دستگاه‌های IoT مقیاس‌پذیر است.

5-4- تحلیل انتقادی

کار پیشنهادی برای بهبود عملکرد شبکه IoT در نظر گرفته شده است. شبکه IoT با مشکلات متعددی مانند کمبود امنیت، حداقل عمر شبکه، مسیریابی ناامن و غیره مواجه است. تکنولوژی بلاکچین و کنترل‌کننده SDN مبتنی بر GA به صورت ترکیبی برای تأمین ارتباطات شبکه و افزایش عمر شبکه استفاده می‌شوند. بلاکچین برای LRA و RCM استفاده می‌شود. مکانیزم LRA منابع کمی مصرف می‌کند زیرا اندازه پیام کمتر است. با این حال، مدارک کم ممکن است باعث حملات جعل هویت، جعل و سیبل شود. این حملات می‌توانند با روش بروت‌فورس انجام شوند. در مکانیزم MND، ما به

```
root@69b8c49be88b:/home# python /oyente/oyente/oyente.py -s LRA_RCM.sol
WARNING:root:You are using evm version 1.8.2. The supported version is 1.7.3
WARNING:root:You are using solc version 0.4.21, The latest supported version is 0.4.19
INFO:root:contract LRA_RCM.sol:LRA_RCM:
INFO:symExec:    ============ Results ===========
INFO:symExec:      EVM Code Coverage:                    99.6%
INFO:symExec:      Integer Underflow:                    False
INFO:symExec:      Integer Overflow:                     False
INFO:symExec:      Parity Multisig Bug 2:                False
INFO:symExec:      Callstack Depth Attack Vulnerability: False
INFO:symExec:      Transaction-Ordering Dependence (TOD): False
INFO:symExec:      Timestamp Dependency:                 False
INFO:symExec:      Re-Entrancy Vulnerability:            False
INFO:symExec:    ====== Analysis Completed ======
```

FIGURE 8. Formal analysis using Oyente tool.

حمله سیاهچاله پرداخته و اطمینان از تحویل بالای بسته‌ها را داریم. با این حال، در این مدل تهدیدات بیشتری مانند حمله انکار سرویس، حمله بازپخش، حمله حفره خاکستری و غیره ممکن است رخ دهد. علاوه بر این، مسیریابی مبتنی بر GA نیاز به زمان زیادی برای محاسبه مسیر دارد که گاهی اوقات برای شبکه به دلیل نیازهای ارتباطی در زمان واقعی غیرقابل قبول است. علاوه بر این، در بلاکچین، تراکنش‌ها زمان قابل توجهی برای اعتبارسنجی نیاز دارند.

5- تجزیه و تحلیل رسمی امنیتی

تحلیل رسمی طرح پیشنهادی از طریق پیاده‌سازی انجام شده است. این طرح به طور خاص برای شناسایی گره‌های مخرب طراحی شده است. این طرح شامل دو بخش اصلی است: مکانیزم شناسایی حمله سیاهچاله که در شبکه اصلی پیاده‌سازی شده و لیست MNL که بر روی بلاکچین نگهداری می‌شود و از طریق ابزار Oyente تحلیل می‌شود. نتایج در شکل (8) نشان داده شده است.

5-1- حمله سیاهچاله

در این بخش، جزئیات استراتژی ما برای مقابله با حمله سیاهچاله را ارائه می‌دهیم، همانطور که در شکل 9 نشان داده شده است. حمله سیاهچاله یا حمله افت بسته زمانی رخ می‌دهد که یک گره بسته را دریافت می‌کند و آن را تایید نمی‌کند. به طور معمول، زمانی که یک گره بسته سلام را به همسایه خود ارسال می‌کند، در مقابل یک بسته تاییدیه دریافت می‌کند. برای بررسی مقاومت طرح پیشنهادی ما، حمله سیاهچاله را با در نظر گرفتن یکی از گره‌ها در مسیر انتخاب شده به عنوان گره مخرب القا می‌کنیم. زمانی که گره مخرب بسته سلام را دریافت می‌کند، بسته تاییدیه را به گره منبع ارسال نمی‌کند. اگر یک گره پس از دریافت پنج بسته سلام، بسته تاییدیه را به گره منبع ارسال نکند، به عنوان گره مخرب شناخته شده و شناسه آن بر روی بلاکچین ذخیره می‌شود. دلیل نگهداری لیست بر روی بلاکچین جلوگیری از دستکاری داده‌ها است.

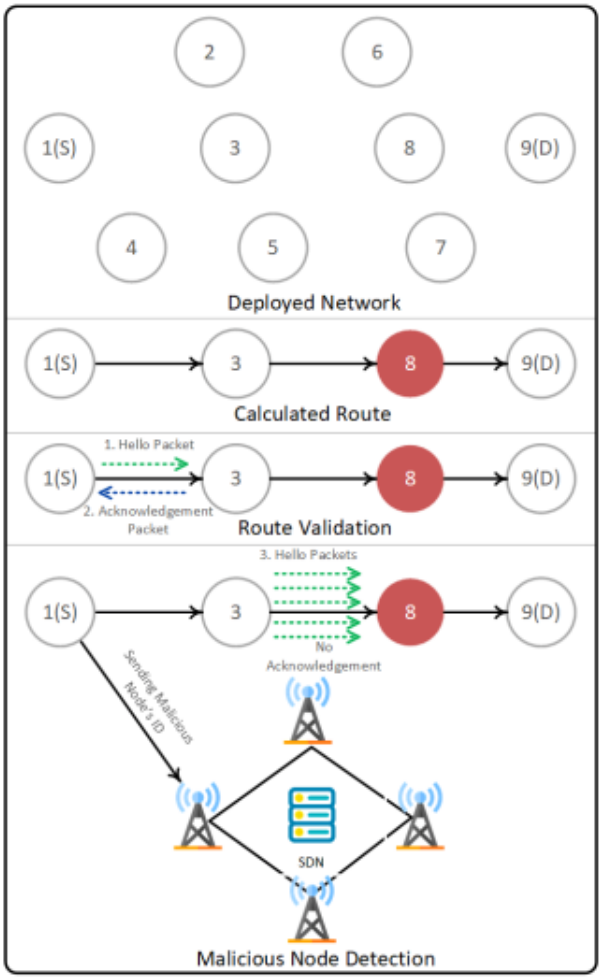


FIGURE 9. Proposed attacker model against black hole attack.

5-2- تحلیل قرارداد هوشمند

برای نگهداری لیست MNL بر روی بلاکچین، از یک قرارداد هوشمند استفاده می‌شود که به زبان برنامه‌نویسی Solidity نوشته شده است. قراردادهای هوشمند تراکنش‌های امن بین گره‌های مختلف را بدون دخالت شخص ثالث امکان‌پذیر می‌کنند. با این حال، به دلیل روش‌های برنامه‌نویسی نامناسب، قراردادهای هوشمند ممکن است در برابر حملات مختلفی مانند حمله DAO، حمله بازگشتی، حمله ترتیب تراکنش و غیره آسیب‌پذیر شوند.

ما قرارداد هوشمند خود را با استفاده از ابزار تحلیل Oyente مورد بررسی قرار دادیم. Oyente یک ابزار متن‌باز است که قرارداد هوشمند را به صورت نمادین اجرا می‌کند تا آسیب‌پذیری‌های بحرانی را شناسایی کند. شکل 8 تحلیل Oyente از قرارداد هوشمند پیشنهادی ما را نشان می‌دهد. مشخص است که قرارداد هوشمند ما در برابر همه آسیب‌پذیری‌های شناخته‌شده قراردادهای هوشمند ایمن است. برخی از آسیب‌پذیری‌های قرارداد هوشمند که به طرح ما مربوط می‌شوند به شرح زیر بحث شده‌اند.

5-2-1- حمله بازگشتی

در یک حمله بازگشتی، یک کاربر مخرب ممکن است اجرای عادی یک تابع قرارداد هوشمند را مختل کرده و همان تابع را چندین بار با استفاده از پارامترهای مختلف بدون خطا اجرا کند. قرارداد هوشمند در طرح پیشنهادی ما شناسه‌های گره‌های مخرب را در لیست MNL ذخیره می‌کند. با این حال، این تابع فقط توسط گره‌های مجاز قابل اجرا است. این محدودیت از افزودن اطلاعات نادرست به لیست MNL توسط کاربران مخرب جلوگیری می‌کند.

5-2-2- وابستگی به زمان‌سنج

در این حمله، مهاجم زمان‌بندی بلوک‌ها را دستکاری می‌کند تا اطلاعات نادرست به دفتر کل اضافه کند. از آنجایی که هیچ تابع وابسته به زمان در قرارداد هوشمند ما وجود ندارد، بنابراین طرح ما در برابر این حمله ایمن است.

5-2-3- حمله انباشت تماس

در این حمله، مهاجم به طور مکرر توابع قرارداد هوشمند خارجی را فراخوانی می‌کند تا از 1024 تماس فراتر برود. پس از آن، تماس‌های تابع عادی به دلیل رسیدن به حد مجاز شکست خواهند خورد. در طرح ما، این حمله ممکن نیست زیرا قرارداد هوشمند پیشنهادی ما هیچ تابع خارجی ندارد.

5-2-4- اشکال چند امضایی Parity

این حمله به کاربران مخرب اجازه می‌دهد تا مالکیت حساب قربانی را به دست گیرند. در نتیجه، مهاجم می‌تواند وجوه آن حساب را سرقت کند و توابعی را که فقط برای کاربران مجاز محفوظ است اجرا کند. با این حال، نتایج Oyente نشان می‌دهد که قرارداد هوشمند پیشنهادی ما در برابر این حمله ایمن است.

5-2-5- وابستگی به ترتیب تراکنش‌ها

در این حمله، یک ماینر مخرب ممکن است سعی کند ترتیب تراکنش‌ها را به‌طور مخرب تغییر دهد تا عملکرد استاندارد قرارداد را مختل کند. این حمله زمانی رخ می‌دهد که قرارداد هوشمند دارای توابعی باشد که به ترتیب تراکنش‌ها وابسته باشند. این حمله در قرارداد هوشمند پیشنهادی ما ممکن نیست زیرا هیچ‌کدام از توابع قرارداد هوشمند وابستگی به ترتیب تراکنش ندارند. علاوه بر این، ماینرهای موجود در طرح پیشنهادی ما نهادهای معتمد هستند؛ بنابراین، حتی اگر این آسیب‌پذیری وجود داشته باشد، این حمله رخ نخواهد داد.

6- نتیجه گیری

در این مقاله، بلاکچین برای ذخیره اعتبار گره‌ها به منظور دستیابی به مقاومت در برابر دستکاری و ناشناس ماندن جهت اطمینان از اعتماد و حریم خصوصی در شبکه توزیع شده، پیاده‌سازی شده است. یک مکانیزم LRA پیشنهاد شده است که در آن اعتبارها بر روی بلاکچین ذخیره می‌شوند تا در فرآیند مسیریابی مورد استفاده قرار گیرند. کنترل‌کننده SDN فعال شده با GA برای محاسبه مسیرها بین گره مبدا و مقصد استفاده می‌شود که منجر به بهینه‌سازی مصرف انرژی گره‌های واسط (RNs) می‌شود. کنترل‌کننده SDN از اعتبارهای از پیش ذخیره شده گره‌ها برای محاسبه مسیر استفاده می‌کند. پس از محاسبه مسیر، مسیر به بلاکچین برای اعتبارسنجی از طریق قرارداد هوشمند RCM ارسال می‌شود. RCM مسیر را با لیست MNL (ایجاد شده پس از شناسایی گره‌های مخرب جدید) مقایسه می‌کند. اگر هر یک از گره‌های مسیر در MNL وجود داشته باشد، بلاکچین درخواست مسیر را مجدداً به کنترل‌کننده SDN ارسال می‌کند؛ در غیر این صورت، مسیر به گره مبدا ارسال می‌شود. علاوه بر این، یک مکانیزم MND مبتنی بر تاییدیه پیشنهاد شده است که بدکاری یا مرگ گره‌های واسط را شناسایی می‌کند. این روش به گره مبدا اجازه می‌دهد تا گره‌های مخرب یا مرده را از طریق پیام سلام سبک‌وزن شناسایی کند که منجر به کاهش مصرف انرژی می‌شود. گره مبدا پیام سلام را به گره همسایه ارسال می‌کند. اگر تاییدیه دریافت نشود، پیام سلام پنج بار دیگر ارسال می‌شود؛ در غیر این صورت، ارتباط آغاز می‌شود. در صورتی که هیچ تاییدیه‌ای دریافت نشود، گره مبدا گره مربوطه را به عنوان مخرب اعلام کرده و شناسه آن را در MNL اضافه می‌کند. نتایج شبیه‌سازی نشان می‌دهد که مدل پیشنهادی ما از نظر مصرف گاز، تعداد بسته‌های افتاده و انرژی باقی‌مانده گره‌ها مؤثر است. مدل پیشنهادی نیاز به هزینه‌های کمتر اجرایی و تراکنشی برای ثبت‌نام و احراز هویت گره‌های واسط دارد. در آینده، قصد داریم مکانیزم مسیریابی را از طریق تکنیک‌های فرابتکاری مختلف انجام دهیم. علاوه بر این، ما مکانیزم MND و محاسبه مسیر را با استفاده از تکنیک‌های یادگیری ماشین بهبود خواهیم داد. همچنین، قصد داریم یک مدل مهاجم را با در نظر گرفتن حملات سیبل، حملات جعل هویت، حملات انکار سرویس و غیره، پیاده‌سازی کنیم.

مراجع

[1] Accessed: Sep. 15, 2021. [Online]. Available: https://iot-analytics.com/ state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-forthe-first-time/

[2] Z. Ming and M. Xu, ‘‘NBA: A name-based approach to device mobility in industrial IoT networks,’’ *Comput. Netw.*, vol. 191, May 2021, Art. no. 107973.

[3] I. Mohiuddin, H. Almajed, Z. Abubaker, A. Almogren, N. Javaid, and T. N. Qureshi, ‘‘Attack resistance-based topology robustness of scale-free Internet of Things for smart cities,’’ *Int. J. Web Grid Services*, vol. 17, no. 4, p. 343, 2021.

[4] A. Shahid, A. Almogren, N. Javaid, F. A. Al-Zahrani, M. Zuair, and M. Alam, ‘‘Blockchain-based Agri-food supply chain: A complete solution,’’ *IEEE Access*, vol. 8, pp. 69230–69243, 2020.

[5] N. Javaid, A. Sher, W. Abdul, I. Niaz, A. Almogren, and A. Alamri,

[20] S. Nakamoto, ''Bitcoin: A peer-to-peer electronic cash system,'' Tech. Rep., 2008.

[21] B. Mohankumar and K. Karuppasamy, ''Network lifetime improved optimal routing in wireless sensor network environment,'' *Wireless Pers. Commun.*, vol. 117, no. 4, pp. 3449–3468, Apr. 2021.

[22] D. V. Medhane, A. K. Sangaiah, M. S. Hossain, G. Muhammad, and J. Wang, ''Blockchain-enabled distributed security framework for nextgeneration IoT: An edge cloud and software-defined network-integrated approach,''*IEEEInternetThingsJ.*,vol.7,no.7,pp. 6143–6149,Jul.2020.

[23] H. Gao, X. Qin, R. J. D. Barroso, W. Hussain, Y. Xu, and Y. Yin, ''Collaborative learning-based industrial IoT API recommendation for softwaredefined devices: The implicit knowledge discovery perspective,'' *IEEE Trans. Emerg. Topics Comput. Intell.*, early access, Sep. 29, 2020, doi: 10.1109/TETCI.2020.3023155.

[24] X. Shi, Y. Li, H. Xie, T. Yang, L. Zhang, P. Liu, H. Zhang, and Z. Liang, ''An Openflow-based load balancing strategy in SDN,'' *C. Mater. Contin.*, vol. 62, Jan. 2020, Art. no. 38520.

[25] C. Guo, J. Guo, C. Yu, Z. Li, C. Gong, and A. Waheed, ''A safe and reliable routing mechanism of LEO satellite based on SDN,'' *Comput., Mater. Continua*, vol. 64, no. 1, pp. 439–454, 2020.

[26] J. Cheng, J. Li, N. Xiong, M. Chen, H. Guo, and X. Yao, ''Lightweight mobile clients privacy protection using trusted execution environments for blockchain,'' *Comput., Mater. Continua*, vol. 65, no. 3, pp. 2247–2262, 2020.

[27] R. Goyat, G. Kumar, M. K. Rai, R. Saha, R. Thomas, and T. H. Kim, ''Blockchain powered secure range-free localization in wireless sensor networks,'' *Arabian J. Sci. Eng.*, vol. 45, no. 8, pp. 6139–6155, Aug. 2020.

[28] T.-H. Kim, R. Goyat, M. K. Rai, G. Kumar, W. J. Buchanan, R. Saha, and R. Thomas, ''A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks,'' *IEEE Access*, vol. 7, pp. 184133–184144, 2019.

[29] K. Haseeb, N. Islam, A. Almogren, and I. Ud Din, ''Intrusion prevention framework for secure routing in WSN-based mobile Internet of Things,'' *IEEE Access*, vol. 7, pp. 185496–185505, 2019.

[30] W.She,Q.Liu,Z.Tian,J.-S.Chen,B.Wang,andW.Liu,''Blockchaintrust model for malicious node detection in wireless sensor networks,'' *IEEE Access*, vol. 7, pp. 38947–38956, 2019.

[31] Y. Huang, H. Xu, H. Gao, X. Ma, and W. Hussain, ''SSUR: An approach to optimizing virtual machine allocation strategy based on user requirements for cloud data center,'' *IEEE Trans. Green Commun. Netw.*, vol. 5, no. 2, pp. 670–681, Jun. 2021.

[32] S. Rathore, B. W. Kwon, and J. H. Park, ''BlockSecIoTNet: Blockchainbased decentralized security architecture for IoT network,'' *J. Netw. Comput. Appl.*, vol. 143, pp. 167–177, Oct. 2019.

[33] M. H. Kumar, V. Mohanraj, Y. Suresh, J. Senthilkumar, and G. Nagalalli, ''Trust aware localized routing and class based dynamic block chain encryption scheme for improved security in WSN,'' *J. Ambient Intell. Humanized Comput.*, vol. 12, no. 5, pp. 5287–5295, May 2021.

''Cooperative opportunistic pressure based routing for underwater wireless sensor networks,'' *Sensors*, vol. 17, no. 3, p. 629, Mar. 2017.

[6] N. Javaid, ''NADEEM: Neighbor node approaching distinct energyefficient mates for reliable data delivery in underwater WSNs,''

Trans. Emerg. Telecommun. Technol., Dec. 2019, Art. no. e3805, doi: 10.1002/ett.3805.

[7] M. V. O. de Assis, L. F. Carvalho, J. J. P. C. Rodrigues, J. Lloret, and M. L. Proença, Jr., ''Near real-time security system applied to SDN environments in IoT networks using convolutional neural network,'' *Comput. Electr. Eng.*, vol. 86, Sep. 2020, Art. no. 106738, doi: 10.1016/j.compeleceng.2020.106738.

[8] N. Javaid, M. Ejaz, W. Abdul, A. Alamri, A. Almogren, I. Niaz, and N. Guizani, ''Cooperative position aware mobility pattern of AUVs for avoiding void zones in underwater WSNs,'' *Sensors*, vol. 17, no. 3, p. 580, Mar. 2017.

[9] S. Yousefi, F. Derakhshan, H. S. Aghdasi, and H. Karimipour, ''An energyefficient artificial bee colony-based clustering in the Internet of Things,'' *Comput. Electr. Eng.*, vol. 86, Sep. 2020, Art. no. 106733.

[10] M. Wazid, A. K. Das, V. Bhat, and A. V. Vasilakos, ''LAM-CIoT: Lightweight authentication mechanism in cloud based IoT environment,'' *J. Netw. Comput. Appl.* vol. 150, Jan. 2020, Art. no. 102496.

[11] L. Vishwakarma and D. Das, ''SCAB–IoTA: Secure communication and authentication for IoT applications using blockchain,'' *J. Parallel Distrib. Comput.*, vol. 154, pp. 94–105, Aug. 2021.

[12] G. Yang, L. Dai, and Z. Wei, ''Challenges, threats, security issues and new trends of underwater wireless sensor networks,'' *Sensors*, vol. 18, no. 11, p. 3907, Nov. 2018.

[13] S. A. Rahman, H. Tout, C. Talhi, and A. Mourad, ''Internet of Things intrusion detection: Centralized, on-device, or federated learning?'' *IEEE Netw.*, vol. 34, no. 6, pp. 310–317, Nov. 2020.

[14] G. Kolumban-Antal, V. Lasak, R. Bogdan, and B. Groza, ''A secure and portable multi-sensor module for distributed air pollution monitoring,'' *Sensors*, vol. 20, no. 2, p. 403, Jan. 2020.

[15] Z.Cui, F.XUE,S.Zhang, X.Cai,Y.Cao, W.Zhang,andJ. Chen,''Ahybrid BlockChain-based identity authentication scheme for multi-WSN,'' *IEEE Trans. Services Comput.*, vol. 13, no. 2, pp. 241–251, Apr. 2020.

[16] J. Yang, S. He, Y. Xu, L. Chen, and J. Ren, ''A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks,'' *Sensors*, vol. 19, no. 4, p. 970, Feb. 2019.

[17] J. Li, S. Hu, Y. Shi, and C. Zhang, ''A blockchain based trustable framework for IoT data storage and access,'' in *Proc. Int. Conf. Blockchain Trustworthy Syst.* Singapore: Springer, 2019, pp. 336–349.

[18] X. Feng, J. Ma, Y. Miao, Q. Meng, X. Liu, Q. Jiang, and H. Li, ''Pruneable sharding-based blockchain protocol,'' *Peer Peer Netw. Appl.*, vol. 12, no. 4, pp. 934–950, Jul. 2019.

[19] H.Lazrag,R.Saadane,andM.D.Rahmani,''Ablockchain-basedapproach for optimal and secure routing in wireless sensor networks,'' in *Proc. 1st Int. Conf. Comput. Sci. Renew. Energies*, Nov. 2018, pp. 411–415.

IoT sensors,'' *IEEE Commun. Lett.*, vol. 24, no. 1, pp. 183–187, Jan. 2020.

[50] H. Feng, W. Wang, B. Chen, and X. Zhang, ''Evaluation on frozen shellfish quality by blockchain based multi-sensors monitoring and SVM algorithm during cold storage,'' *IEEE Access*, vol. 8, pp. 54361–54370, 2020.

[51] G. R. Harik, F. G. Lobo, and D. E. Goldberg, ''The compact genetic algorithm,'' *IEEE Trans. Evol. Comput.*, vol. 3, no. 4, pp. 287–297, Nov. 1999.

[52] S. K. Gupta, P. Kuila, and P. K. Jana, ''GAR: An energy efficient GA based routing for wireless sensor networks,'' in *Proc. Int. Conf. Distrib. Comput. Internet Technol.* Berlin, Germany: Springer, 2013, pp. 267–277.

[53] B. Ghaleb, A. Al-Dubai, E. Ekonomou, M. Qasem, I. Romdhani, and L. Mackenzie, ''Addressing the DAO insider attack in RPL's Internet of Things networks,'' *IEEE Commun. Lett.*, vol. 23, no. 1, pp. 68–71, Jan. 2019.

[54] A. Alkhalifah, A. Ng, P. A. Watters, and A. S. M. Kayes, ''A mechanism to detect and prevent Ethereum blockchain smart contract reentrancy attacks,'' *Frontiers Comput. Sci.*, vol. 3, p. 1, Feb. 2021.

[55] C. Liu, H. Liu, Z. Cao, Z. Chen, B. Chen, and B. Roscoe, ''ReGuard: Finding reentrancy bugs in smart contracts,'' in *Proc. 40th Int. Conf. Softw. Eng., Companion*, May 2018, pp. 65–68.

[56] B. K. Mishra, M. C. Nikam, and P. Lakkadwala, ''Security against black hole attack in wireless sensor network—A review,'' in *Proc. 4th Int. Conf. Commun. Syst. Netw. Technol.*, Apr. 2014, pp. 615–620.

[34] G. Ramezan and C. Leung, ''A blockchain-based contractual routing protocol for the Internet of Things using smart contracts,'' *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–14, Nov. 2018.

[35] A. Moinet, B. Darties, and J.-L. Baril, ''Blockchain based trust & authentication for decentralized sensor networks,'' 2017, *arXiv:1706.01730*. [Online]. Available: http://arxiv.org/abs/1706.01730

[36] S. Hong, ''P2P networking based Internet of Things (IoT) sensor node authentication by blockchain,'' *Peer-to-Peer Netw. Appl.*, vol. 13, no. 2, pp. 579–589, Mar. 2020.

[37] G. Rathee, M. Balasaraswathi, K. P. Chandran, S. D. Gupta, and C. S. Boopathi, ''A secure IoT sensors communication in industry 4.0 using blockchain technology,'' *J. Ambient Intell. Humanized Comput.*, vol. 12, no. 1, pp. 533–545, Jan. 2021.

[38] B. Jia, T. Zhou, W. Li, Z. Liu, and J. Zhang, ''A blockchain-based location privacy protection incentive mechanism in crowd sensing networks,'' *Sensors*, vol. 18, no. 11, p. 3894, Nov. 2018.

[39] Y. Guo, H. Xie, Y. Miao, C. Wang, and X. Jia, ''FedCrowd: A federated and privacy-preserving crowdsourcing platform on blockchain,'' *IEEE Trans. Services Comput.*, early access, Oct. 14, 2020, doi: 10.1109/ TSC.2020.3031061.

[40] Y. Tian, Z. Wang, J. Xiong, and J. Ma, ''A blockchain-based secure key management scheme with trustworthiness in DWSNs,'' *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 6193–6202, Sep. 2020.

[41] P. K. Sharma and J. H. Park, ''Blockchain based hybrid network architecture for the smart city,'' *Future Gener. Comput. Syst.* vol. 86, pp. 650–655, Sep. 2018.

[42] Y. Liu, K. Wang, Y. Lin, and W. Xu, ''LightChain: A lightweight blockchain system for industrial Internet of Things,'' *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3571–3581, Jun. 2019.

[43] I. Azam, N. Javaid, A. Ahmad, W. Abdul, A. Almogren, and A. Alamri, ''Balanced load distribution with energy hole avoidance in underwater WSNs,'' *IEEE Access*, vol. 5, pp. 15206–15221, 2017.

[44] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasurbramanian, ''A lightweight blockchain based framework for underwater IoT,'' *Electronics*, vol. 8, no. 12, p. 1552, Dec. 2019.

[45] S. Kushch and F. Prieto-Castrillo, ''A rolling blockchain for a dynamic WSNs in a smart city,'' 2018, *arXiv:1806.11399*. [Online]. Available: http://arxiv.org/abs/1806.11399

[46] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung, and M. Song, ''Computation offloading and content caching in wireless blockchain networks with mobile edge computing,'' *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11008–11021, Nov. 2018.

[47] P. Danzi, A. E. Kalor, C. Stefanovic, and P. Popovski, ''Delay and communication tradeoffs for blockchain systems with lightweight IoT clients,'' *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2354–2365, Apr. 2019.

[48] Y. Ren, Y. Liu, S. Ji, A. K. Sangaiah, and J. Wang, ''Incentive mechanism of data storage based on blockchain for wireless sensor networks,'' *Mobile Inf. Syst.*, vol. 2018, pp. 1–10, Aug. 2018.

[49] A. Rovira-Sugranes and A. Razi, ''Optimizing the age of information for blockchain technology with applications to